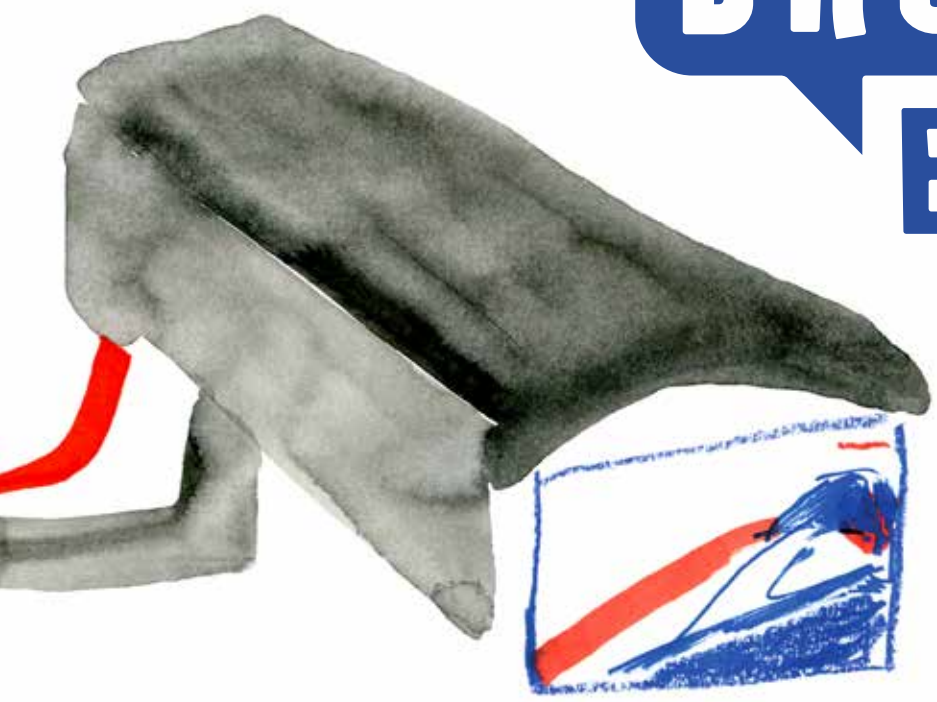
BRUXELLES EN MOUVEMENTS

Bimestriel,
Paraît 6 fois par an
Bureau de dépôt :
Bruxelles X
P 302402

bpost
PB-PP | B-01148
BELGIE(N) - BELGIQUE

PÉRIODIQUE ÉDITÉ PAR
INTER-ENVIRONNEMENT-BRUXELLES,
FÉDÉRATION DE COMITÉS DE QUARTIER
ET GROUPES D'HABITANT·ES

N°332 – SEPTEMBRE/OCTOBRE 2024



DANS L'ŒIL DU NUMÉRIQUE

INTRODUCTION

DES MÉTADONNÉES & DES HUMAINS

La multiplication des pratiques de surveillance dans la ville interroge. D'autant que les ambitions de Bruxelles à s'imposer comme une *smart city* se sont, jusqu'à présent, presque exclusivement matérialisées dans le domaine sécuritaire. Il est donc temps de passer en revue ces pratiques, parfois nouvelles, et de donner la parole à celles et ceux qui analysent de près leur mise en place, l'interrogent ou la combattent.

Inter-Environnement Bruxelles

La surveillance peut se définir comme « la collecte et l'analyse d'informations sur des individus ou des groupes afin de régir leur activité »[1]. Dans cette acception, la pratique est aussi ancienne que les premières formes d'organisations étatiques – et des guerres qu'elles ont menées. Ce qui est nouveau, c'est l'explosion de la quantité d'informations collectées, en particulier ces dernières années, avec les évolutions de l'informatique.

Aujourd'hui, chaque individu se trouve quotidiennement au centre de la production d'un nombre colossal de données : images de caméras, localisation, opérations bancaires, utilisation de carte MoBIB, antécédents médicaux, historique de navigation web, activités sur les médias sociaux, connexions aux réseaux wifi, pétitions signées, langues pratiquées, visas délivrés… et tant d'autres donnant des informations liées au bagage culturel de la personne, à son état psychique, à ses caractéristiques physiques, etc.

Toutes ces données ne sont bien sûr pas enregistrées avec comme objectif premier de nous surveiller. Beaucoup le sont par simple nécessité technique, ou pour nous offrir un meilleur confort dans l'utilisation de services. Isolées, la plupart de ces données peuvent d'ailleurs paraître bien anodines. Cependant, combinées entre elles, ces masses d'information sont de plus en plus à même de circonscrire, de manière relativement précise, le profil d'un individu. Et ce profil peut-être utilisé par une pluralité d'acteur·ices aux motivations diverses de la police aux compagnies d'assurances, en passant par les multinationales, supermarchés et autres publicitaires. Sans oublier votre employeur, ni vos ancien·nes partenaires en colère !

Si ces tendances inquiètent, elles ne trouvent pas que des détracteur·ices. Dans l'article « Petit pays, Big Data », vous découvrirez que pour lutter contre la criminalité, certain·es voudraient voir la police devenir « prédictive » et « intelligente ». L'efficacité de nos forces de l'ordre devrait à présent dépendre d'algorithmes et de bases de données, remodelant par là même le paysage de la prévention et de la répression.

> Aujourd'hui, chaque individu se trouve quotidiennement au centre de la production d'un nombre colossal de données.

L'outil principal de cette transformation serait la vidéosurveillance, liée aux aménagements urbains défensifs. L'article « La vidéosurveillance à Bruxelles : trop n'est jamais assez » démontre qu'à Bruxelles les autorités poursuivent inlassablement le déploiement de caméras de plus en plus sophistiquées (bodycams, drones, algorithmiques, etc.). Mais les caméras peuvent être subjectives, de mauvaise qualité, non fonctionnelles, inégalement placées dans certains quartiers, etc. C'est ce que rappelle l'article « Vidéosurveillance et violence policière : un champ obstrué », qui souligne également qu'après des années de déploiement sous diverses latitudes, l'efficacité de la vidéosurveillance n'a toujours pas pu être démontrée, particulièrement lorsqu'il s'agit de prévenir, de constater voire de condamner des violences policières.

Plutôt que de contribuer à une amélioration de la vie urbaine, les caméras de surveillance « intelligentes » semblent surtout entretenir le stigmate sur certains groupes sociaux et certaines zones de la ville, mettant en danger au passage nos libertés fondamentales. L'article « La vie privée, pour quoi faire ? » invoque le droit à la vie privée, en particulier à l'aune d'appels de plus en plus pressants à l'instauration de la reconnaissance faciale. Et le texte « La *Sousveillance* : production d'un contrechamp face aux violences policières » rappelle, plus concrètement, que le contre-pouvoir se situe aujourd'hui davantage du côté de la société civile, avec les images de sousveillance filmées au téléphone par des passant·es ou des victimes, et diffusées sur les réseaux sociaux ou dans des journaux indépendants.

SOMMAIRE DU NUMÉRO

Introduction ..... p. 2
La Vidéosurveillance à Bruxelles : trop n'est jamais assez ..... p. 3-6
Vidéosurveillance et violence policière : un champ obstrué ..... p. 7-9
La Sousveillance *: production d'un contrechamp face aux violences policières* ..... p. 11-13
Petit pays, Big Data – Le développement de la police « prédictive » en Belgique ..... p. 14-16
Quand la technologie s'empare de la conversation ..... p. 17-19
Petit guide de résistance numérique ..... p. 20-21
Démocratie & numérique : comment reprendre la main ? ..... p. 22-25
La Vie privée, pour quoi faire ? Exigence démocratique et reconnaissance faciale ..... p. 26-27
Édito : *Pour une Renolution publique du bâti bruxellois* ..... p. 28

Nous avons des connaissances bien inégales en matière de technologie et selon nos affinités avec l'informatique, les enjeux soulevés par la surveillance peuvent nous échapper. L'article « Démocratie & numérique : comment reprendre la main ? » rappelle cependant que les enjeux de surveillance posent des questions d'ordre social qui dépassent les choix techniques et pour lesquelles les débats devraient être ouverts au plus grand nombre. C'est pourquoi le Mouton Numérique s'efforce de sortir le débat technologique du seul cercle des ingénieur·es.

Et parmi les outils que nous utilisons au quotidien, les logiciels de messagerie instantanée sont particulièrement générateurs de données sensibles qui intéressent tout autant les commerciaux, que les institutions judiciaires ou policières. Pour ces dernières instances, le contrôle de nos conversations doit aider à lutter contre différents trafics illégaux et combattre les réseaux criminels. Cependant, l'article « Quand la technologie s'empare de la conversation » rappelle que non seulement l'efficacité d'une telle surveillance reste à prouver, mais qu'en plus elle pose des questions pressantes sur la surveillance croissante de nos vies.

> Les enjeux de surveillance posent des questions d'ordre social qui dépassent les choix techniques.

Pour finir sur une note un peu plus positive, le « Petit guide de résistance numérique » vous invite à suivre les pas de militant·es attentif·ves aux enjeux techniques, afin de découvrir des alternatives à vos applications préférées. Beaucoup d'applications n'échappent en effet pas au paradoxe de nous rendre à la fois plus autonomes, en nous permettant de faire plus de choses, mais également plus dépendant·es de ceux qui développent et distribuent les logiciels. ❏

1. Wiktionary.org

➪ Si Inter-Environnement Bruxelles a pu souffler ses 50 ans cette année, c'est en partie grâce à votre soutien financier ! Alors, n'hésitez pas à continuer. Il nous permet d'animer le débat démocratique à Bruxelles et à faire connaître les multiples facettes des dossiers urbains. Vos dons, autant appréciés qu'utiles, contribuent à assurer l'indépendance de l'association.

Comment ?

● **De préférence via un formulaire accessible sur notre site** [https://www.ieb.be/Soutenez-IEB], **sous forme de don unique ou, mieux encore, mensuel*!**

● **Ou par un versement sur le compte bancaire TRIODOS** BE63 5230 8136 6608 **au nom d'Inter-Environnement Bruxelles, rue du Chimiste 34-36, 1070 Bruxelles.**

* La formule mensuelle nous offre un soutien plus stable. Si le total de vos dons sur l'année civile en cours atteint ou dépasse 40 €, vous bénéficiez d'une déduction fiscale de 45 % sur le montant de votre don. Attention, veillez à bien mentionner vos coordonnées postales en communication pour obtenir une attestation fiscale.

* Les détails de nos actions et de nos budgets apparaissent dans nos rapports d'activités annuels, consultables sur notre site.

VIDÉOSURVEILLANCE À BRUXELLES

TROP N'EST JAMAIS ASSEZ [1]

Les caméras à Bruxelles, cela fait longtemps qu'elles nous observent. Elles seraient désormais « intelligentes »… rien de moins sûr, ni de plus inquiétant.

Alice Querel, Maud Girault et Corentin Debailleul[2]

La caméra du coin de la rue, celle au-dessus de l'épaule de la caissière, sur la poitrine du policier, au milieu du tram ou sur le panneau de signalisation… nous nous sommes peu à peu habitué·es à voir notre paysage urbain se munir de toutes ces tumeurs, rondes, plates, noires ou blanches, selon leur fonction. Elles se déploient, se développent depuis longtemps déjà mais désormais équipées de nouveaux outils de traitement de données : détection des comportements jugés suspects, reconnaissance faciale et autre. Loin de la neutralité technologique brandie, la répartition géographique des caméras, le développement de la reconnaissance faciale ou des algorithmes prédictifs, portent des enjeux fondamentalement politiques.

BREF RETOUR HISTORIQUE

Les caméras de vidéosurveillance apparaissent dans l'espace public bruxellois en 1968, installées par la STIB dans le métro. Elles se développent progressivement au cours des décennies suivantes, à des fins de régulation du trafic routier, ou à l'occasion d'événements pour lesquels la sécurité est renforcée, à l'image du championnat d'Europe de football en 2000 par exemple. C'est à partir de 2003 que les caméras se répandent de façon massive dans la ville, avec la mise en place d'une subvention régionale d'un total de 1,5 million d'euros, pour les communes qui souhaitent développer la vidéosurveillance sur leur territoire. À l'exception d'Auderghem et de Watermael-Boitsfort, toutes les communes bruxelloises bénéficient alors de cette subvention. Entre 2006 et 2015, le nombre de caméras de surveillance dans la Région de Bruxelles-Capitale passe de 192 à 796. Si les premières installations sont le fait des communes, le contrôle des caméras passe rapidement sous la responsabilité des zones de police. En mars 2014, le gouvernement régional vote l'adoption d'un projet de « zone intégrée », qui prévoit l'implantation de plus de 3 000 caméras de surveillance. En 2016, une étude cartographie 1 365 caméras de surveillance dans l'espace public de la Région de Bruxelles-Capitale [3]. 984 sont alors gérées par les services de police communaux, et 378 par le service public des transports MOBIRIS (dont 348 dans les tunnels). À cela s'ajoutent 1 800 caméras installées par la STIB dans les infrastructures du métro (en plus de 4 000 caméras dans les rames), et 62 qui couvrent les zones du port et du canal. D'après les informations recueillies par la Ligue des droits humains dans le cadre d'une campagne de collecte de données [4], on compte en 2022 environ 1 200 caméras de police. De leur côté, les communes ont développé des programmes de lutte contre les dépôts d'ordures, et recourent désormais à des caméras temporaires pour tenter de capturer des images qui pourraient ensuite servir à donner des amendes [5].

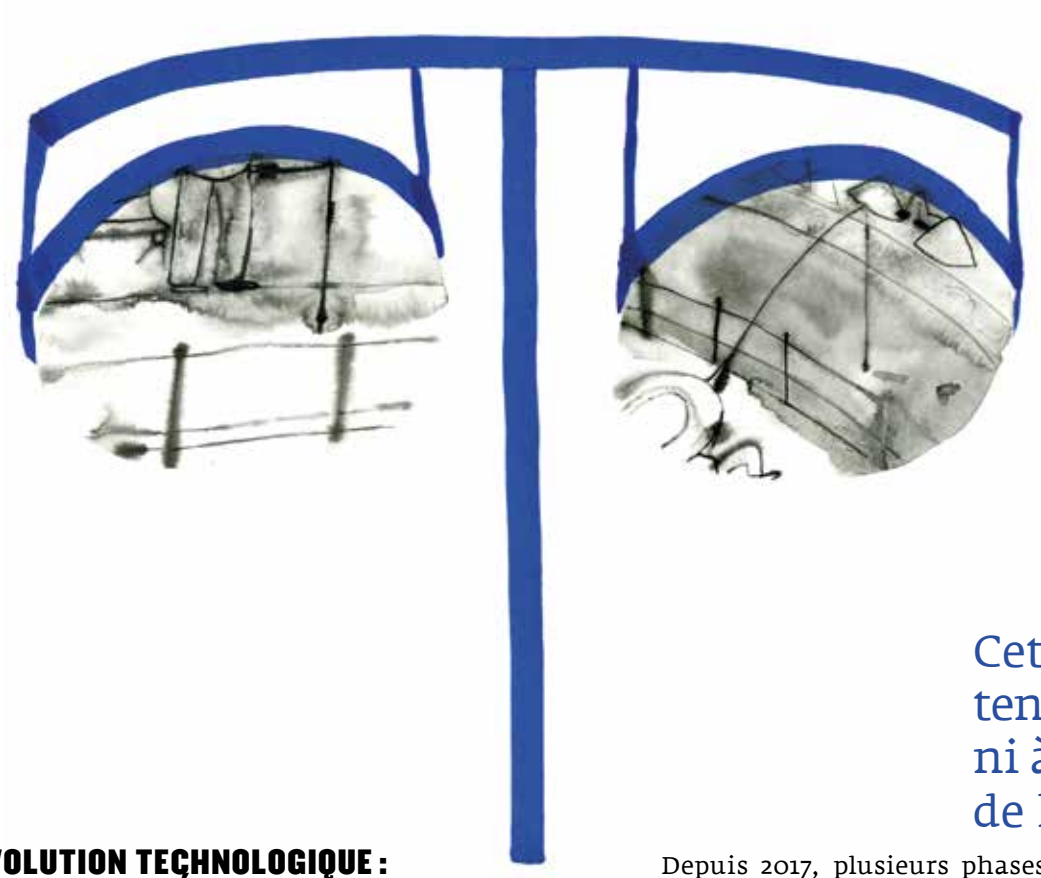
> La vidéosurveillance coûte cher aux collectivités qui décident de la mettre en place.

> En dix ans, le nombre de caméras de surveillance dans la Région de Bruxelles-Capitale a quadruplé.

DES ENJEUX ÉCONOMIQUES MAJEURS

« Une caméra coûte entre 8000 et 27 000 euros, mais d'autres coûts doivent être pris en compte : la consultance utilisée par 60 % des municipalités, l'installation, le fonctionnement et la maintenance. [6] »

À titre d'exemple, le plan en quatre phases prévoyant l'installation de 230 caméras entre 2005 et 2015 dans la zone de police de Bruxelles-Capitale Ixelles avait un budget de plus de 10 millions d'euros, et le dispositif de 130 caméras déployé en 2016 dans la zone de police de Bruxelles-Nord a coûté six millions d'euros. La vidéosurveillance coûte cher aux collectivités qui décident de la mettre en place. Néanmoins les communes en assument rarement la charge seules, et bénéficient de subventions régionales, fédérales, voire européennes. Du côté des fabricants, la vidéosurveillance représente un vaste marché financier au niveau mondial, avec une croissance annuelle de 12,5 % en moyenne. Au total, les recettes mondiales du secteur sont estimées à 81,7 milliards de dollars en 2024 et devraient atteindre 145,4 milliards d'ici 2029 [7].



ÉVOLUTION TECHNOLOGIQUE : VERS DES CAMÉRAS « INTELLIGENTES »

L'expansion de la vidéosurveillance est indissociable d'évolutions technologiques en plein essor : nouveaux appareils (drones, bodycams), ou nouveaux outils de traitement des données (reconnaissance faciale, algorithmes prédictifs).

Au moment des grands plans de déploiement de la vidéosurveillance des années 2010, commencent à apparaître des caméras dites « intelligentes », qui peuvent être associées à des logiciels d'analyse du contenu vidéo programmés pour détecter les comportements jugés suspects. Ainsi, une trop longue immobilité dans un parking peut être analysée comme un potentiel vol de voiture, ou un attroupement de personnes comme une émeute en puissance. Il semblerait néanmoins que ces technologies promettent plus qu'elles n'accomplissent réellement, et que, suscitant un trop grand nombre de fausses alertes, les opérateurs·rices de caméras finissent par s'en désintéresser.

À l'heure actuelle, les seules caméras de surveillance autorisées à être reliées à des fichiers de données personnelles sont les ANPR (pour *automatic number plate recognition*, soit à reconnaissance automatique de plaque d'immatriculation), dont l'installation a été généralisée par la « zone de basses émissions » mise en place en 2018 par la Région de Bruxelles-Capitale et interdisant la circulation des voitures jugées trop polluantes.

> L'effet dissuasif de la vidéosurveillance n'est pas démontré.

Depuis 2017, plusieurs phases de test de vidéosurveillance à reconnaissance faciale ont aussi été effectuées par la police fédérale (la premièrr ayant été lancée à l'aéroport de Bruxelles-National suite aux attentats du 22 mars 2016), alors même que cette technologie n'est pas autorisée en Belgique. Elles ont pour la plupart été stoppées à la suite d'un avis négatif de l'organe de contrôle de l'information policière (COC), et de résultats peu probants concernant les marges d'erreur. Comme le souligne la coalition d'associations à l'origine de la pétition « pour interdire la reconnaissance faciale dans l'espace public bruxellois » du 14 mars 2023 :

> *« D'après une recherche menée par la KULeuven en Flandre et en Région bruxelloise, au moins 5 zones de police locale sur 86 répondantes disposaient de la reconnaissance faciale, l'une d'elles affirmant même l'utiliser "souvent à très souvent". [...] L'usage de la reconnaissance faciale n'est donc pas légal en Belgique mais il persiste dans le chef de la police et de la ministre de l'Intérieur une volonté d'utiliser cette technologie* [8]*. »*

LUTTER CONTRE L'INSÉCURITÉ ?

Selon ses promoteurs, le développement de la vidéosurveillance répond à une logique de lutte contre l'insécurité, cherchant à dissuader, prévenir, mais aussi punir les actes de délinquance. Cette politique ne tend pas à comprendre ni à traiter les causes de l'insécurité, mais bien à y remédier à l'aide d'innovations technologiques, et de techniques urbanistiques ou architecturales. Liées au développement de la vidéosurveillance, les théories de la « prévention situationnelle » [9], ou encore de l'« urbanisme défensif », désignent des politiques d'aménagement de l'espace public qui visent à rendre les villes plus sûres, à la fois en décourageant les comportements criminels, et en renforçant la responsabilisation des habitants et le contrôle social. À Bruxelles, cette approche s'incarne dans certains éléments de mobilier urbain (bancs conçus pour empêcher les gens d'y passer la nuit) ou lors d'opérations de rénovation urbaine, qui réduisent les recoins (supprimer les arbres, créer de grandes esplanades ouvertes minéralisées, comme sur la place Flagey, la place Jourdan, ou le Parvis de Saint-Gilles), permettant aux caméras d'avoir un champ de vision plus opérationnel et de faciliter les interventions des forces de l'ordre.

Toutefois, même en se plaçant dans cette logique sécuritaire, l'efficacité de la vidéosurveillance sur la lutte contre l'insécurité reste incertaine.

L'effet dissuasif de la vidéosurveillance n'est pas démontré, et dépend des types d'espaces : si elle peut avoir un certain impact dans des lieux clos (parkings ou commerces), elle en a très peu dans les espaces extérieurs, étendus et complexes.

Son efficacité a posteriori, dans le cadre de poursuites judiciaires, n'est pas davantage probante [10], les images étant la plupart du temps soit non versées au dossier, soit partielles, soit inexistantes. Lorsqu'elles sont versées au dossier, c'est du reste sous la forme d'un rapport papier où figurent des captures d'écran commentées par les policier·es en charge de l'enquête, ce qui biaise leur lecture [11].

> Cette politique ne tend pas à comprendre ni à traiter les causes de l'insécurité.

On peut légitimement se demander si cette expansion de la vidéosurveillance ne vient pas plus répondre à des logiques politiciennes, notamment balisées par les temps électoraux, qu'agir effectivement sur l'insécurité, devenant un outil d'affichage politique.

> *« Que l'objectif soit d'agir contre la pollution ou l'insécurité, le développement de la vidéosurveillance et d'autres objets "smart" semble plus relever du "solutionnisme technologique" [Morozov, 2014] que d'une mesure politique prenant en compte la complexité des enjeux en présence dans le cadre d'un débat public* [12]*. »*

VIDÉOSURVEILLANCE ET INÉGALITÉS SOCIALES

Le développement de la vidéosurveillance reproduit et entretient les inégalités sociales et raciales à plusieurs niveaux : dans la manière dont est conçue et répartie cette technologie, mais aussi dans celle dont sont traitées ces images. En étudiant les localisations des caméras à Bruxelles, on voit apparaitre une répartition géographique reflétant les inégalités sociales au sein de la population, et une utilisation de la vidéosurveillance visant à protéger des intérêts particuliers et surveiller des groupes sociaux bien précis. Les quartiers bruxellois qui concentrent le plus de caméras de surveillance sont les plus défavorisés sur le plan socio-économique, avec les taux de chômage les plus importants ou les plus fortes proportions de population immigrée (Molenbeek, Matongé). Ils sont d'autant plus équipés qu'ils sont proches du centre-ville, « commercial et touristique », et du quartier européen, eux-mêmes très fournis en caméras. Le nombre de caméras décroît fortement vers le sud-est de la ville : les quartiers plus riches d'Auderghem, Watermael-Boitsfort et Uccle ne font l'objet que d'une faible vidéosurveillance publique. ➡

Ainsi, certaines populations sont particulièrement filmées, notamment les populations pauvres et racisées, ce qui pousse certain·es auteur·es à parler de « profilage ethnique » :

> *« Le profilage ethnique recouvre une multiplicité de mécanismes structurels et s'opère lorsque des activités de contrôle, de surveillance et d'investigation ne sont pas basées sur des motifs raisonnables mais sur la couleur de peau, l'origine ou la religion supposées ou réelles* [13]. »

Certains outils en développement, comme la bodycam ou la reconnaissance faciale, risquent d'accentuer ces pratiques discriminatoires. Plusieurs biais ont été relevés par des chercheur·euses, l'un des plus notoire étant que les hommes blancs sont surreprésentés dans les bases de données utilisées pour entrainer les algorithmes et que de nombreux « faux positifs » apparaissent lorsque ces algorithmes sont appliqués à d'autres populations (personnes racisées, femmes, etc.), des erreurs qui peuvent mener en prison. La mise en lien de la vidéosurveillance et d'algorithmes prédictifs, censés identifier des lieux à risques par exemple, pourrait aggraver ce phénomène de profilage ethnique :

> *« La surexposition des jeunes issus de l'immigration postcoloniale et en particulier dans les quartiers populaires, ainsi que divers mécanismes discriminatoires (biais des technologies, préjugés, quadrillage racialisé des dispositifs, etc.) entraînent un biais dans ces banques de données à la base des activités dites prédictives* [14]. »

À rebours de certaines stratégies de légitimation de la vidéosurveillance qui mettent en avant une supposée neutralité technologique, on peut également souligner les stéréotypes véhiculés par les agent·es en charge du traitement des images de vidéosurveillance. Dans une étude réalisée en 1990 [15], les chercheurs Norris et Armstrong ont montré que les opérateurs qui analysaient les images de vidéosurveillance ciblaient en priorité des adolescents masculins, et que l'appartenance réelle ou supposée à un groupe ethnique était un critère déterminant. Par ailleurs, environ la moitié des « personnes ciblées » l'étaient sans « aucune raison évidente » permettant de justifier *a priori* l'intervention des opérateur·ices, celle-ci reposant alors principalement sur leurs préjugés.

DES PRINCIPES FONDAMENTAUX MIS DE CÔTÉ

Les multiples usages de la vidéosurveillance bafouent un certain nombre de principes sans que soient réellement mises au débat public ces évolutions. Sont remis en question des droits et libertés fondamentaux comme le droit de circuler ou de se réunir librement dans l'espace public, le droit au respect de la vie privée, à l'anonymat, ou encore la présomption d'innocence. Certains développements en cours font craindre des dérives plus importantes encore, en particulier l'utilisation de la reconnaissance faciale :

> *« Cette technologie implique d'importants risques : piratages de données à caractère personnel très sensibles, erreurs et reproduction des discriminations sexistes ou racistes induites par les conceptions sociales dominantes et les institutions qui les vendent et qui les utilisent, menace d'un glissement vers une surveillance de masse* [16]. »

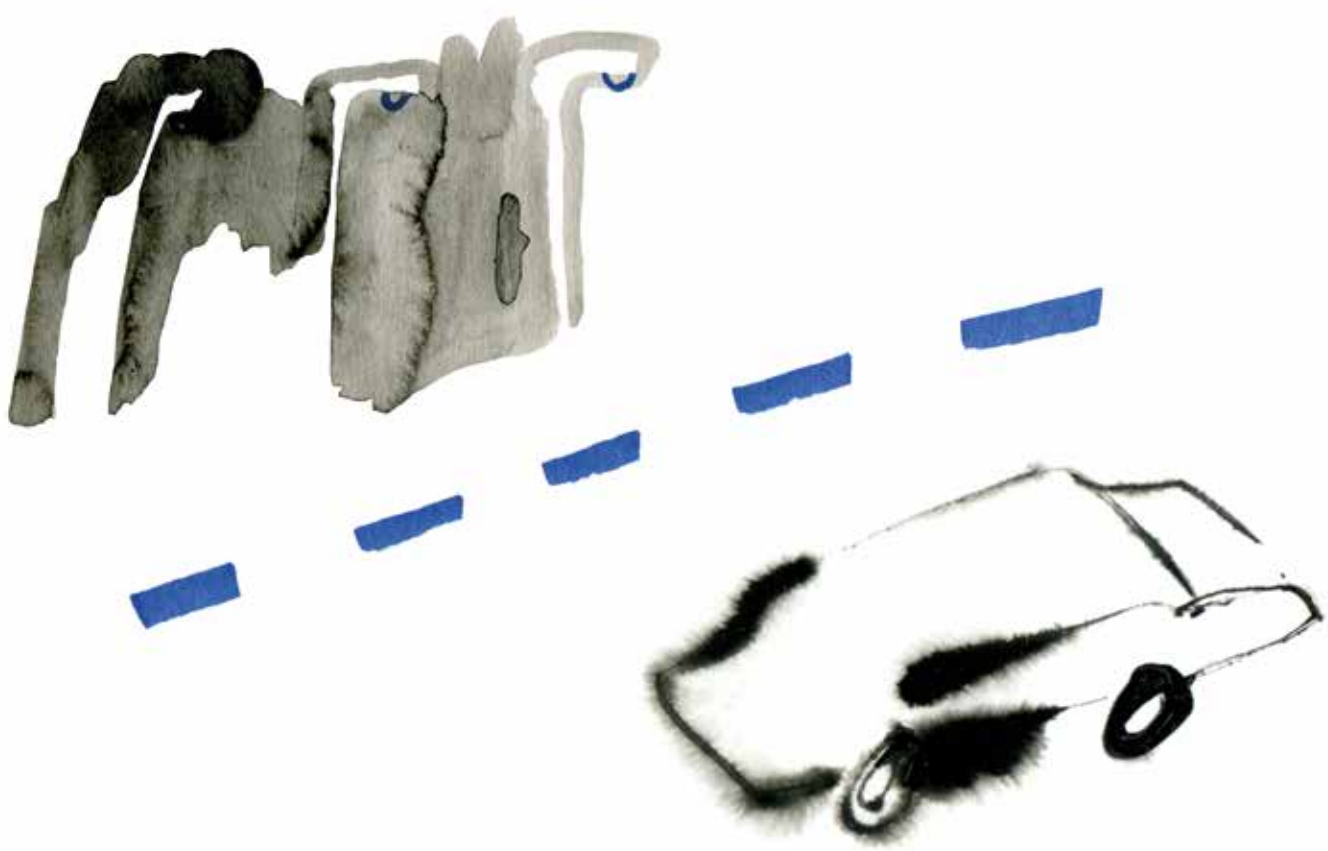
POUR CONCLURE…

À Bruxelles, la police, les communes et la Région poursuivent inlassablement le déploiement de caméras de plus en plus sophistiquées. Les raisons pour lesquelles ces caméras sont mises en place ont elles aussi évolué : à écouter certaines déclarations de responsables politiques, on pourrait croire que les caméras sont à même de résoudre tous les problèmes. Pourtant, rien n'est moins sûr. L'efficacité de la vidéosurveillance, étudiée depuis plusieurs années et sous diverses latitudes, n'est toujours pas démontrée. Plutôt que de contribuer à une amélioration de la vie urbaine, les caméras de surveillance « intelligentes » semblent surtout entretenir le stigmate sur certains groupes sociaux et certaines zones de la ville, mettant en danger au passage droit à la vie privée et autres libertés fondamentales. Au fond, la question qu'on est en droit de se poser est la suivante : si les caméras font pire que mieux, pourquoi en sommes-nous encore là ? ❑

> Les quartiers bruxellois qui concentrent le plus de caméras de surveillance sont les plus défavorisés sur le plan socio-économique.

> Les multiples usages de la vidéosurveillance bafouent un certain nombre de principes sans que soient réellement mises au débat public ces évolutions.

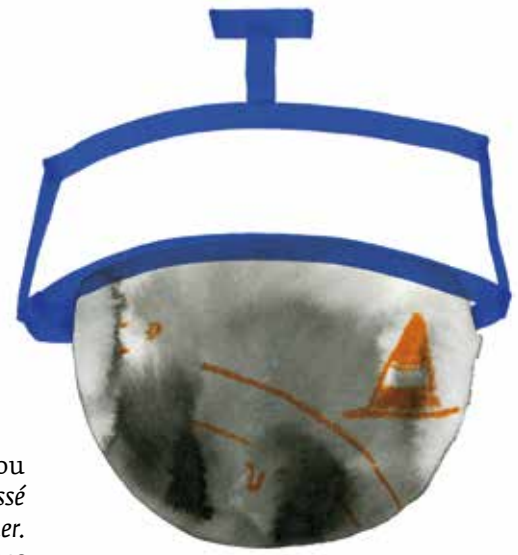
1. Une précédente version de ce texte est parue sur le site surveillances.be. Il s'appuie notamment sur le travail de P. DE KEERSMAECKER et C. DEBAILLEUL, « Répartition géographique de la vidéosurveillance dans les lieux publics de la Région de Bruxelles-Capitale », *Brussels Studies*, n° 104, 10 octobre 2016.
2. Merci à Sarah De Laet pour ses relectures et contributions.
3. DE KEERSMAECKER et DEBAILLEUL, *op. cit.*
4. E. DE HOUCK, « Transparence administrative et vidéosurveillance : certains communes et zones de police sont parfois bien silencieuses », *rtbf.be*, 12 mai 2022.
5. https://transparencia.be/request/decisions_et_registres_sur_les_d_98#incoming-5627
6. Ces chiffres sont issus d'une étude Markets & Markets, citée par la Ligue des Droits Humains, « Sous l'œil de la sécurité : la vidéosurveillance dans l'espace public », 2019.
7. Mordor Intelligence, « Analyse de la taille et de la part du marché de la vidéosurveillance – Tendances de croissance et prévisions (2024-2029) » [https://www.mordorintelligence.com].
8. https://democratie.brussels/initiatives/i-155
9. Concept forgé par l'architecte et urbaniste O. NEWMAN, dans son ouvrage *Defensible Space: People and Design in the Violent City,* Architectural Press, 1972.
10. ÉLODIE LEMAIRE, *L'Œil sécuritaire : mythes et réalités de la vidéosurveillance*, éd. La Découverte, 2019.
11. Voir « Vidéosurveillance et violence policière : un champ obstrué », p. 7-9.
12. La Ligue des Droits Humains (2019), art. cit.
13. R. FARGE, « Police du futur et nouvelles technologie du profilage ethnique », Chronique de la Ligue des Droits Humains, 2019.
14. F. BACCHINI, L. LORUSSO, « Race, again: how face recognition technology reinforces racial discrimination », *Journal of Information, Communication and Ethics in Society*, 2019, p. 321-335.
15. E. HEILMANN, « La vidéosurveillance et le travail policier », in Devresse et Piéret (dir.) *La vidéosurveillance. Entre usages politiques et pratiques policières*, éd. Politeia, 2009, p. 127-134.
16. « Une pétition pour interdire la reconnaissance faciale dans l'espace public bruxellois », 14 mars 2023 [https://www.liguedh.be].



VIDÉOSURVEILLANCE ET VIOLENCE POLICIÈRE UN CHAMP OBSTRUÉ[1]

Quand les images de vidéosurveillance sont convoquées dans des affaires où les policiers sont impliqués : un cas d'école de l'aporie du système juridico-policier.

Maud Girault



La législation belge définit ainsi la vidéosurveillance : « *On entend par caméra de surveillance tout système d'observation fixe ou mobile qui collecte, traite ou sauvegarde des images dans le but de prévenir, constater ou déceler les délits*[2]. »

Quel est le rôle et la fonction des caméras de surveillances dans les affaires de violences policières, donc de policier·es possiblement incriminé·es ? « Prévenir » et « constater » pour condamner… Vraiment ?

> Sourour Abouda, Mohamed Amine Berkane, Ilyes Abbedou, Ibrahima Barrie, Joseph Chovanec, Simon Bachelard, Dieumerci Kanda, Jonathan Jacob, Hassan Chrikri…

PRÉVENIR ?

Les images ne sont pas regardées en direct : Sourour Abouda, Mohamed Amine Berkane, Ilyes Abbedou, Ibrahima Barrie, Joseph Chovanec, Simon Bachelard, Dieumerci Kanda, Jonathan Jacob, Hassan Chrikri : tout·es sont mort·es en cellule devant des caméras de surveillance.

La plupart de ces décès restent aujourd'hui inexpliqués. Les policiers invoquent souvent des malaises ou des suicides qui auraient alors eu lieu sous l'œil des caméras, ne suscitant aucune réaction des policier·es. « *On filme, mais on regarde pas ce qu'on filme !* » déclare l'avocat Vincent Lurquin. Il raconte, à propos d'Ilyes Abbedou (2021, Bruxelles) : « *On l'a laissé toute la nuit, on l'a laissé jusqu'à 15h. À 9h du matin on lui a donné son petit déjeuner. Moi j'ai vu les films, vous voyez très précisément qu'il n'a pas bougé depuis qu'il est là, on le voit pendant des heures et des heures… et on lui apporte son petit déjeuner. Et on va lui rechercher son petit déjeuner qu'il n'a pas mangé… puisqu'il était mort*[3] *!* »

Le service de dispatching qui aurait dû regarder les images des caméras de surveillance de la cellule dans laquelle s'est pendu Dieumerci Kanda le 7 février 2015 surveillait aussi les 150 caméras de rue de la zone de police Midi, rapporte le journal *Médor*[4]. Cette surenchère de caméras et l'impossibilité de les regarder toutes en direct peut être une des pistes de compréhension de l'absence de réaction des policier·es.

Des violences commises sous l'œil des caméras : D'autres personnes ont été frappées à mort par la police malgré la présence de caméras et de collègues qui pouvaient les regarder. Pensons à Jonathan Jacobs, mort des suites des coups reçus dans sa cellule anversoise en 2010, ou à Joseph Chovanec, qui a été maintenu par un plaquage ventral durant 16 minutes dans sa cellule, pendant qu'une policière faisait un salut nazi à l'aéroport de Charleroi en 2018. Ils et elle ne semblaient nullement se soucier d'être filmé·es, et leurs collègues du dispatching ne sont en effet pas intervenu·es. La présence de caméras n'a pas dissuadé les policier·es. Ces violences commises sous l'œil des caméras reflètent un fort sentiment d'impunité de la part des policier·es.

Dans toutes ces affaires, les caméras de surveillance n'ont nullement permis de prévenir : elles n'ont pas servi à secourir des personnes qui avaient besoin d'aide alors qu'elles étaient enfermées sous la responsabilité de la police, ni empêché des policier·es de frapper ou de tuer.

> Ces violences commises sous l'œil des caméras reflètent un fort sentiment d'impunité de la part des policier·es.

CONSTATER ?

Des images non lisibles : Pour « constater » un délit, il faudrait avoir accès à des images satisfaisantes. Pourtant, souvent, les caméras présentent des cadrages non pertinents. Contrairement à une caméra présente pour cadrer une situation, comme c'est le cas lorsqu'un témoin filme avec son téléphone, les caméras de surveillance sont installées au préalable et sont souvent fixes. La scène n'est pas cadrée, et bien souvent, une partie de ce qui s'y joue se passe en hors-champ, en dehors du cadre de la caméra. En outre, le champ de la caméra s'avère souvent partiellement bouché par un premier plan (une camionnette, des arbres, etc.) empêchant une analyse précise de la situation.

Des images qui disparaissent : Il est troublant de voir que les caméras qui auraient pu incriminer des policier·es dans les affaires de violences policières ne fonctionnaient souvent pas. Caméras non branchées, cassées, images écrasées, problème d'horodateur, vidéos avec des sautes… ce sont des situations très courantes aux dires des avocat·es et familles de victimes. ➡

Ainsi, les images des onze minutes qui précèdent la mort de Soulaïmane Archich Jimili ont disparu. Il avait été écrasé par le métro en 2014 à Bruxelles suite à un contrôle policier. Il avait quinze ans. Youssef Archich, son oncle, raconte être allé voir les images au commissariat avec le père de Soulaïmane. Les policier·es leur ont d'abord montré les images d'une caméra dont l'axe ne permettait pas de voir l'interpellation des jeunes gens sur le quai du métro. On n'y voyait Soulaïmane qu'à la fin de la scène, au moment où il est écrasé par le métro. La famille voulait savoir ce qu'il s'était passé avant. Ils ont finalement pris connaissance des images issues d'une autre caméra, sur lesquelles on pouvait voir Soulaïmane être interpellé par les policier·es et agent·es de la STIB. Des images soudainement coupées : « *Les onze minutes de vidéo qui étaient les plus compromettantes pour les policiers, puisqu'ils rentrent physiquement en contact avec les enfants : on les voit pas. La STIB a répondu simplement que ces images avaient été écrasées, sans aucune autre explication. On ne voit que ce qu'ils ont bien voulu nous laisser voir* », témoigne Youssef Archich [5].

Vincent Lurquin, l'avocat de la famille de Moad Touile, qui a été tabassé par la police en 2013 alors qu'il avait quatorze ans, nous raconte également comment des images ont subitement disparu : « *J'ai été voir ce qu'il en était par rapport à ces caméras du commissariat. Parce que dès que vous entrez il y a une caméra qui vise la sortie, et toutes les cellules sont filmées. Moad avait dit qu'il avait reçu des coups encore là-bas. Les policier·es disaient que ce n'était pas vrai.* [...] *Alors on a regardé et j'étais embêté parce qu'effectivement, cellule par cellule, il n'y avait rien. Mais moi j'avais quand même tendance à croire mon client, je me disais "Pourquoi il m'a raconté ça ? Il avait déjà sa semelle..."* [une marque de semelle laissée au visage, attestée par un médecin]. *Alors je fais attention. En dessous vous avez le timecode et je vois qu'entre deux cellules, entre le moment où on le fouille et entre le moment où il est amené à la cellule, il y a douze minutes qui manquent.* »

Un autre avocat montre une vidéo issue de la caméra de surveillance d'un hôtel, vidéo qui avait été saisie dans un dossier de violences policières. Une coupe est visible dans la vidéo. Le PV du comité P. qui décrit l'image stipule : « *Il y a une coupure entre 14h39 et 14h43, soit précisément au moment donné ou l'incident principal serait survenu, étant donné qu'aucune coupure aussi large n'est constatée par la suite à la fin de l'intervention* ».

Cette coupe est expliquée ainsi dans le PV : « *La caméra présente enregistre sous détection de mouvements, ce système n'est pas remarquablement précis et il peut donner lieu à des failles. Dans la période qui nous intéresse, avec les coins d'ombres, la distinction en couleur est moins précise et la détection de mouvements se fait plus difficilement.* »

> « On ne voit que ce qu'ils ont bien voulu nous laisser voir. »

L'avocat récuse cette analyse : « *On voit que là ils restent dans l'ombre et que ça reste filmé...* », il conclut : « *Donc personne ne croit ça.* [...] *Moi j'ai dit au procureur en charge de ce dossier : "Ils ont coupé là dedans, les policiers." Le procureur m'a répondu : "Que voulez-vous que je fasse ? Les policiers me disent qu'il n'y a rien de plus, et que c'est dû à la caméra... je sais rien faire." "Il y a des policiers qui se foutent bien de votre gueule, désolé", je lui ai répondu. Voilà, et c'est classé sans suite.* »

Dans ces affaires comme dans d'autres, il est saisissant de constater que ce sont précisément les minutes de vidéos les plus cruciales pour comprendre ce qu'il s'est passé qui manquent aux enregistrements.

CONDAMNER ?

Les captures d'écran : Les images de vidéosurveillance sont saisies selon l'appréciation du ou de la procureur·e du Roi en charge de l'enquête. Cela peut également faire suite à la demande d'un·e avocat·e de victime de violences policières. Les images peuvent alors être un élément de preuve parmi d'autres, mais c'est sous la forme d'un rapport papier où figurent des captures d'écran commentées par les policier·es en charge de l'enquête qu'elles sont versées au dossier, et c'est de cette manière que les magistrat·es prennent connaissance des vidéos.

> Les images sont alors sélectionnées, figées et interprétées.

Les images sont alors sélectionnées, figées et interprétées. Elles sont assorties d'un commentaire écrit et d'une légende, qui guident nécessairement leur lecture.

Par exemple, on lit dans un PV : « *Un septième policier arrive en marchant* [...] *recule tout en portant sa main à la hanche* » – comment sait-t-on qu'il recule sur une capture d'écran ? A été ajouté un encart fléché qui dirige le regard : « *Policier main à la hanche* ».

Le texte influence toujours l'interprétation de l'image. Avec les captures d'écran commentées présentes dans les PV, la lecture de la vidéo est guidée à plusieurs niveaux : l'image est sélectionnée, extraite de son contexte, fixée, commentée et décrite. Les vidéos sont ainsi relues, réinterprétées. Dans certains PV, il n'y a même pas de capture d'écran, juste une « analyse d'images caméra » écrite.

L'interprétation des images et le « regard blanc » [6] : Cette interprétation des images ne peut s'extraire de son contexte, notamment de rapports de domination marqués par des schèmes racistes et la prégnance d'un regard blanc. Elsa Dorlin en a fait l'analyse à partir des images de l'arrestation de Rodney King (un homme noir tabassé par la police à Los Angeles en 1991). Elle relève que ces images qui furent accueillies comme l'évidence de la violence policière, ont été vues *a contrario* par le jury comme une scène de légitime défense montrant la « vulnérabilité des policiers » face à cet homme noir : « *King ne peut pas être perçu comme un corps qui se défend, il est vu a priori comme un agent de la violence* [7]. »

Les membres du comité « Justice pour Lamine Bangoura » font une lecture similaire et montrent les mécanismes de criminalisation du corps noir pendant l'arrestation et le meurtre de Lamine Bangoura à Roeselare en 2018 [8]. Ce corps est perçu comme ayant une force surhumaine qu'il faut maîtriser. Ils montrent aussi comment cette vision a terni tout le procès. En entendant les râles d'agonie de Lamine Bangoura, sur la vidéo filmée par l'assistant de l'huissier intervenu chez lui, la Cour de cassation de Gand parlera de « rugissements » : « *Pour comprendre qu'une telle lecture de l'image soit possible, il faut tenir compte sérieusement de ce fait : le regard profondément et historiquement raciste qui est posé sur ce corps noir, le regard du blanc. Le regard du blanc, ce n'est pas un acte de perception directe, neutre. Le "rugissement", c'est le résultat d'une production raciale du visible. Celle des policiers qui va convaincre leur avocat qui va convaincre le juge qui va convaincre les journalistes. "Lamine Bangoura, plus Lukaku que Messi", titre* Le Soir. *C'est un regard historiquement façonné par un schème raciste, c'est une manière d'entrer en relation perceptive, esthétique et émotionnelle avec les corps noirs* [9]. »

> En entendant les râles d'agonie de Lamine Bangoura, la Cour de cassation de Gand parlera de « rugissements »...

L'interprétation qui est faite des images par les policier·es est nourrie de ces représentations racistes. Il est alors crucial pour les avocat·es de victime de violences policières d'obtenir les images afin de pouvoir en proposer une contre-analyse.

LA DIFFICULTÉ D'OBTENIR LES IMAGES

L'accès aux images pour les avocat·es de la partie civile est compliqué : il faut réussir à les faire saisir avant qu'elles ne soient effacées, puis réussir à les récupérer au greffe et à les visionner.

Les délais de conservation : Les règles concernant la conservation et l'accès aux images dépendent de s'il s'agit de caméras privées (soumise à la « loi caméra » [10]) ou de caméras « utilisées dans la cadre de missions de police », donc aussi bien les caméras fixes que les caméras mobiles telles que les bodycams, qui sont soumises à la loi sur la fonction de police (LFP) [11].

- Dans le premier cas, le délai maximum de conservation des images est de 30 jours [12].
- Dans le deuxième cas, les images peuvent être conservées maximum 12 mois mais leur accès ne pourra avoir lieu que le premier mois, dans des affaires traitées par la police administrative, 12 mois pour la police judiciaire.

Cependant, ces lois encadrent le temps de conservation maximal des images, non minimal. Très souvent, lorsque les avocat·es en demandent la saisie, ils et elles se voient répondre que les images ont été effacées. Les capacités de stockage des images dans les serveurs de la police expliquent, notamment, pourquoi les temps de conservation sont en réalité très courts.

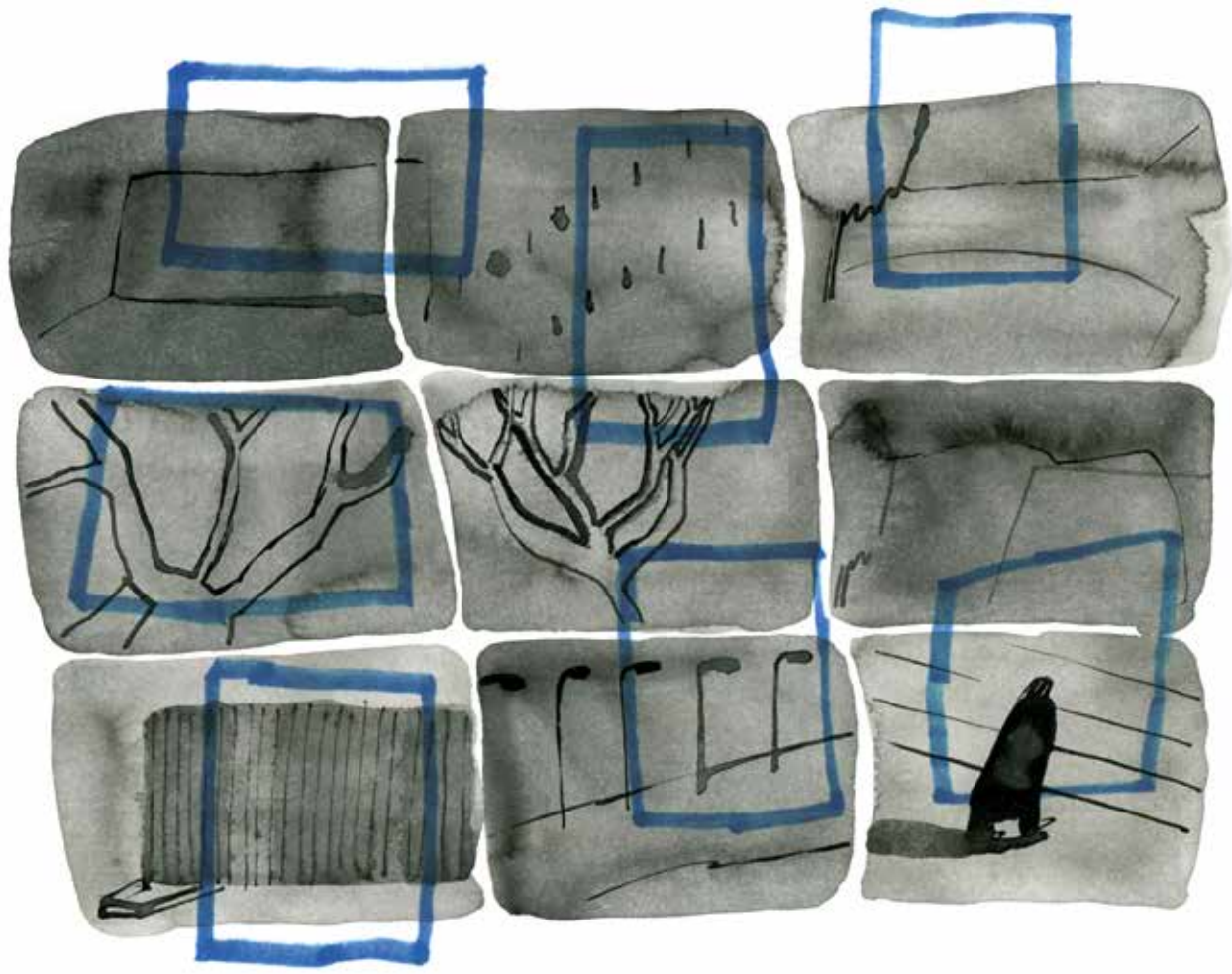
L'obtention des images s'avère ainsi souvent être une course contre la montre. L'avocat Alexis Deswaef raconte : « *C'est le réflexe qu'il faut avoir comme avocat, on dépose une plainte chez le juge d'instruction et il faut en parallèle demander au procureur tout de suite de mettre les images à l'abri, les sauvegarder, parce que souvent ces images ne sont gardées que 30 jours et s'il faut passer par la mise en instruction et les délais que ça prend, les images sont déjà effacées* [13]. »

Le stockage et l'accès aux images : Une fois que les images ont été saisies, encore faut-il que les avocat·es puissent y avoir accès, et c'est également un parcours du combattant. Elles doivent être déposées en tant que pièces à conviction, ce qui est loin d'être la règle.

Une fois que les images sont effectivement au greffe, les avocat·es peuvent aller les consulter. C'est une démarche qui n'est pas courante car elle prend du temps et ne porte pas souvent ses fruits. Nous avons accompagné une avocate au greffe du Tribunal de Police de Bruxelles et avons pu observer les obstacles encore rencontrés à cette étape-ci : c'est sur un CD-ROM que les images avaient été copiées dans un format très peu courant. Après avoir essayé en vain d'installer des logiciels pour ouvrir le CD-ROM sur son ordinateur personnel, l'avocate a demandé l'assistance d'une employée. La vidéo s'est avérée corrompue. L'avocate a alors dû faire reporter l'audience pour demander qu'un nouveau CD-ROM valide soit déposé au greffe. La deuxième fois où elle y est retournée, le CD-ROM était encore corrompu et la vidéo n'était toujours pas visible et l'avocate a dû demander de nouveau un report d'audience.

Un avocat nous explique qu'il y a une incompatibilité informatique entre le système du parquet et celui de la police : le format utilisé pour les fichiers de la police n'est pas compatible avec les ordinateurs du greffe. Il faut alors renvoyer les vidéos pour changer le format. L'avocate Joke Callewaert nous dit à ce propos : « *Le problème c'est qu'il y a plein d'avocats qui ne font pas ces démarches, d'aller voir la vidéo, de pousser auprès du juge pour demander à voir la vidéo parce que ça énerve les juges* [14]. »

Une fois que les images ont été saisies, encore faut-il que les avocat·es puissent y avoir accès.



Le visionnage des vidéos pendant les audiences : Aucun visionnage d'images ou de vidéo n'est prévu pendant les jugements. Il n'y a pas de matériel disponible pour cela en Belgique. Si l'avocat·e de la partie civile souhaite montrer une vidéo, il ou elle devra en faire la demande, ce qui est souvent refusé car le ou la juge estime que cela prendra trop de temps. Si c'est accepté, l'avocat·e doit apporter son propre ordinateur. Avocat·es, juge, greffier·e, procureur·e, etc. se tassent alors derrière l'ordinateur personnel de l'avocat·e pour visionner et écouter la vidéo, avec la qualité que l'on peut imaginer.

ANGLE MORT

> « *Imaginer qu'on va résoudre un problème de société aussi profond que l'impunité de la police avec des trucs techniques… c'est illusoire.* » [Selma Benkhelifa [15]]

Tant du côté de la chaîne technique, que de celui de la chaîne juridique, les obstacles sont nombreux pour que les images policières – issues des caméras de surveillance, mais aussi des bodycams – puissent prévenir ou permettre de constater, voire condamner, des violences policières. Certain·es militant·es évoquent les angles morts des caméras des commissariats ou l'absence de caméras dans les fourgons et dans le local de fouille, mais il nous semble que ce n'est pas la multiplication des caméras qui résoudrait les obstacles inhérents à notre système juridico-policier. Le contre-pouvoir se situe peut-être davantage du côté de la société civile, avec les images de sousveillance filmées au téléphone par des passant·es ou des victimes, et diffusées sur les réseaux sociaux ou dans des journaux indépendants. ❏

Le contre-pouvoir se situe peut-être davantage du côté de la société civile.

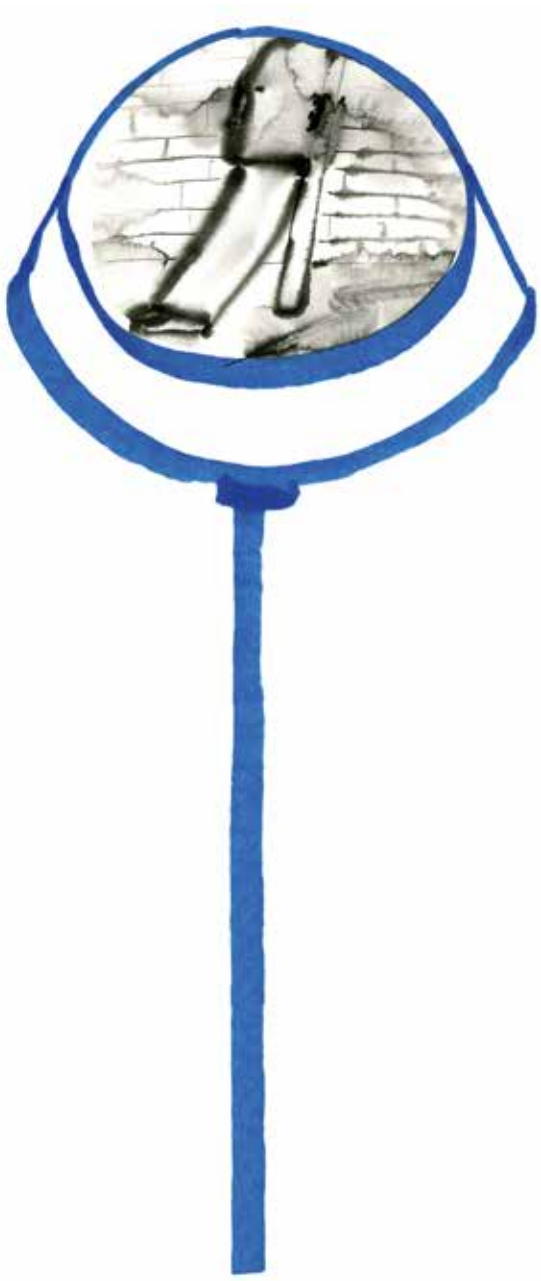
1. Une précédente version de ce texte est parue sur le site surveillances.be. Voir aussi le dossier de Police Watch (LDH) en collaboration avec l'Equality Law Clinic : « L'apport des preuves audiovisuelles en matière de violences policières ».
2. https://www.belgium.be/fr/justice/respect_de_la_vie_privee/surveillance_camera
3. Entretien réalisé le 9 juin 2023.
4. J. MEIJER et P. PEYROLLE, « Autopsie d'une mort étrange en cellule », *Médor*, 2021.
5. « Soulaymane, 2 ans déjà », Radio Rive West, 2016 [https://radiorivewest.wordpress.com/].
6. Expression empruntée à Nordine Saïdi, fondateur de Bruxelles Panthères.
7. E. DORLIN, *Se défendre, Une philosophie de la violence*, éd. Zones, 2017.
8. Lamine Bangoura a été tué à son domicile par huit policiers en 2018, lors d'une expulsion domiciliaire.
9. Comité Justice et Vérité pour Lamine Bangoura, « Déconstruire le regard blanc », par la voix de Nordine Saïdi à la table ronde ronde « Impacts d'image de violences policières prises au Smartphone » organisée au cinéma Nova [Notes synthétiques sur https://surveillances.be/].
10. https://www.besafe.be/fr/loi-camera
11. https://www.besafe.be/fr/loi-camera/lfp-enregistrement-conservation-et-acces-aux-images
12. Ce délai peut être prolongé à trois mois pour des lieux qui peuvent présenter un risque particulier pour la sécurité tels que les gares, les aéroports, les prisons etc.
13. Entretien réalisé le 8 février 2022.
14. Entretien réalisé le 10 mars 2022.
15. Idem.

LA SOUSVEILLANCE

PRODUCTION D'UN CONTRECHAMP FACE AUX VIOLENCES POLICIÈRES [1]

Aujourd'hui des témoins ou des victimes de violence policière utilisent leurs téléphones pour prendre la parole par leurs images. Mais quel est l'impact de ce point de vue longtemps invisible ? Que se passe-t-il quand les surveillés se mettent à surveiller les surveillants ?

Maud Girault



Face au panoptique des caméras policières (caméras de surveillance, bodycams, drones), un contrechamp s'est développé depuis une dizaine d'années, celui des images issues de téléphones brandis par des témoins, des passant·es, des contrôlé·es, des victimes de violences policières. Comment ces images produisent-elles des contre-récits et en quoi ces récits aident-ils face aux violences policières ?

Le *copwatching*, littéralement « regarder/surveiller les flics », désigne la prise de vue et la diffusion d'images de policier·es dans l'exercice de leur fonction. Ce terme renvoie à une pratique développée initialement dans les années 1990 aux États-Unis : des équipes volontaires patrouillaient dans les quartiers pauvres. Elles suivaient la police pour contrôler son action avec des caméras vidéo décorées d'autocollants « Protéger et servir », en référence aux écussons de la police étasunienne.

Depuis 2011 et la généralisation des smartphones, permettant à tout un chacun d'avoir une caméra légère constamment sur soi, la pratique de filmer la police s'est considérablement développée, prenant davantage la forme d'une action individuelle que d'une organisation collective. Un contrechamp se dessine face aux images de surveillance. Steve Mann [2] proposa dès 2006 le terme de « sousveillance » pour qualifier cette dynamique. En filmant les interventions de la police, les contrôlé·es, ou les manifestant·es, se protègent et reprennent un rôle d'acteurs et d'actrices : « *Filmer l'événement introduit certes la menace d'une potentielle visibilité publique, mais elle restitue d'abord à celui ou celle qui subit le contrôle un statut de sujet de droit* [3]. »

> Des Gilets jaunes en France à George Floyd aux États-Unis, ces images sont devenues « l'arme des désarmés ».

Des Gilets jaunes en France à George Floyd aux États-Unis, ces images sont devenues « *l'arme des désarmés* [4] ». Face à cette profusion d'images, l'enjeu réside alors dans le stockage, le recensement et la diffusion de ces images : les invisibles, non seulement se rendent visibles, mais organisent également un contre-récit face au récit de la police, de la justice, des politiques avec la diffusion de ces images. Cet article esquisse les mécanismes qui sous-tendent la construction de ces contre-récits, afin d'en saisir les impacts mais aussi les limites.

LA DIFFUSION DES IMAGES OU LA CONSTRUCTION DE CONTRE-RÉCITS

Les images de violences policières filmées au téléphone par des témoins ou les victimes elles-mêmes portent dans l'espace public une représentation directe des premier·es concerné·es, et nécessitent généralement une collaboration entre différent·es acteur·ices pour toucher une audience conséquente. La manière dont une image est rendue publique contribue à la construction des contre-récits. Ceux-ci n'ont pas les mêmes caractéristiques selon la chaîne de diffusion (réseaux sociaux, journalisme, contre-expertise, etc.) et leurs finalités (sensibiliser l'opinion publique ou contribuer à une procédure judiciaire).

Juridiquement, les images peuvent être constituées comme preuves si elles font partie « *d'un faisceau d'indices convergents* » [5], mais pour notre part nous les abordons comme une trace – avec une construction, des limites techniques et un point de vue situé. Dès lors, à chaque étape de la lecture d'une image, s'opère un travail de reconstitution de la trace au sein d'un récit pour lui conférer un sens, une lecture et une valeur de preuve. Voici trois exemples d'espaces de diffusion de ces images qui induisent des langages et esthétiques différenciés.

LES RÉSEAUX SOCIAUX

Ce ne sont généralement pas les mêmes personnes qui produisent les images et qui permettent leur viralité sur les réseaux sociaux. Le journal *Le Monde* analysait ainsi les images de révolte qui circulaient sur Snapchat suite à la mort de Nahel M., tué par une balle à bout portant tirée par un policier en 2023 en île-de-France : « *Si ces contenus finissent par se répandre en ligne, c'est surtout grâce à certains comptes-clés, qui se chargent d'agréger les vidéos issues des comptes privés* [6]. » Le récit se construit selon les choix « éditoriaux » du compte agrégateur, son activité et son panel de vidéos et selon les métadonnées visibles qui accompagnent la vidéo (commentaire, légende, titre, tag).

> Cette image qui déconstruit le récit mensonger policier et, dans un même mouvement, met en question tous les récits policiers précédents qui invoquaient la légitime défense pour inverser les responsabilités.

LA CONTRE-EXPERTISE À VISÉE SCIENTIFIQUE

En Belgique, le groupe indépendant de recherche Retrace a vu le jour en novembre 2023. À la suite de Forensic Architecture [7] et de l'ONG Index [8], leur objectif est de proposer des contre-enquêtes à partir de sources ouvertes comme les vidéos filmées par des passant·es : « *L'approche contre-forensique dans laquelle nous nous inscrivons tend à inverser la direction du regard forensique officiel afin de le retourner contre les institutions étatiques et contester le quasi-monopole de celles-ci sur les procédures permettant la manifestation de la vérité* [9]. » Ce groupe a ainsi publié en novembre 2023, en collaboration avec le journal *Le Soir*, une enquête vidéo sur les conditions de la mort de Ouassim et Sabrina en 2017. C'est un ensemble de codes avec une esthétique propre qui se développe dans ces contre-enquêtes : les images de *sousveillances* sont intégrées à une vidéo qui inclut des reconstitutions 3D et des documents de l'instruction, le tout guidé par une voix off.

> La manière dont une image est rendue publique contribue à la construction des contre-récits.

LES PROCÉDURES JUDICIAIRES

Dans les procédures judiciaires, les images filmées au téléphone par des passant·es ou par les contrôlé·es sont généralement davantage mobilisées par la partie civile pour essayer de prouver la violence des policier·es, que par les avocat·es des policier·es. Contrairement aux images policières qui arrivent dans les mains des juges sous la forme de captures d'écrans légendées [10], les avocat·es essayent de faire visionner ces vidéos de smartphones pendant l'audience. Mais cela n'est pas réglementé et dépend du bon vouloir du juge, et les avocat·es doivent apporter leur propre matériel car en Belgique les salles ne sont pas pourvues de matériel de projection.

Les vidéos – montrées en audience ou bien jointes au dossier – sont inscrites dans la production du récit judiciaire : les images font partie des éléments mobilisés à charge ou à décharge, et sont soumises à un jeu d'interprétations face aux magistrat·es.

Ces circuits de diffusion (web, journalistiques, judiciaires) ont donc chacun leur moteur et esthétique propres au service de la construction d'un récit. Pour autant, la logique *Open source* à l'œuvre dans ces trois modes de diffusions permettent non seulement que ces images soient accessibles mais aussi de pouvoir remonter à la source de la vidéo (pour vérifier son intégralité, savoir où et qui l'a filmée etc.) contrairement aux images produites par la police. En outre, ces différents usages des vidéos ne s'excluent pas les unes les autres, au contraire, et une affaire qui aura été très relayée grâce à des images virales sur les réseaux sociaux pourra avoir d'autant plus l'attention des magistrat·es si elle est jugée.

> Les images de sousveillance qui arrivent dans les mains des avocat·es aident à disculper les victimes.

QUEL(S) CONTRE-POUVOIR(S) CES CONTRE-RÉCITS PERMETTENT-ILS ?

1. Du côté des tribunaux

« *En Belgique, une personne qui est victime de violence illégitime par des membres des forces de l'ordre se voit souvent dépourvue de voies de recours, les dossiers étant régulièrement classés sans suite ou, lorsqu'ils ne le sont pas, ils n'aboutissent que très rarement à une condamnation* [11]. » Pour autant, sans images, les policier·es sont encore moins condamné·es. C'est ce dont témoigne l'avocat Alexis Deswaef : « *Ça fait plus de 10 ans que je défends des victimes de violences policières et le constat que je porte c'est que les images sont essentielles parce qu'on peut avoir de très bons dossiers, ça sera très difficile d'obtenir la condamnation des policiers en question s'il n'y a pas d'images* [12]. »

Les vidéos de *sousveillances* ont l'avantage d'être accessibles pour la partie civile contrairement aux images de vidéosurveillance (bodycams, drones, caméras de surveillance), et si les policier·es sont rarement condamné·es, ces images permettent, *a minima*, d'ouvrir des instructions ou de disculper les victimes des fausses accusations dont elles font généralement les frais.

Ouvrir une instruction : Avril 2020, alors que Bruxelles était encore confinée, A.J., un migrant soudanais sans-papiers, a été violemment agressé par des policiers. Il a été frappé pendant son arrestation puis dans le fourgon des policier·es. Le traçage GPS a par ailleurs montré que ces derniers ont cherché une place sombre et discrète pour le relâcher, puis l'ont encore gazé. Il y a fort à parier que le statut de A.J. aurait encore davantage contribué à l'invisibilisation de ces violences. Mais elles ont été filmées et un « compte agrégateur » a rapidement diffusé la vidéo sur les réseaux sociaux. Le bourgmestre de Bruxelles est intervenu pour demander qu'une instruction soit ouverte. La saisie des téléphones et l'analyse des comptes WhatsApp des policiers ont montré que les policiers se sont accordés sur un récit mensonger des événements. L'avocat de A.J., Alexis Deswaef, commente : « *Je crois que la médiatisation et le fait que ça a été mis sur Facebook ont forcé le Procureur à réagir et la police a tout de suite ouvert une enquête disciplinaire. Ça a suscité beaucoup d'émoi… le bourgmestre s'est saisi du dossier, et c'est clair que ça a joué, s'il y avait pas eu ça, peut-être qu'on n'en aurait jamais parlé.* » La Cour d'appel correctionnelle de Bruxelles a condamné en mars 2022 le policier incriminé à un an de prison avec sursis et 1 600 € d'amende. ➡

Les images ont dans ce cas permis qu'il y ait une enquête. Si la peine prononcée peut paraître légère, chaque condamnation de policier·es représente malgré tout un précédent en Belgique.

Disculper d'accusations de rébellion : Systématiquement, pour se protéger, les policier·es portent plainte contre les personnes qu'iels frappent. L'avocate Joke Callewaert explique : « *En fait, la plupart des dossiers dans le cas de violences policières, ce sont des dossiers de jeunes qui sont poursuivis pour rébellion après avoir subi des coups de la part des flics.* [...] *Ce ne sont pas des peines très lourdes, mais elles ouvrent un casier* [13]. » Généralement, des personnes poursuivies pour rébellion s'inscrivent dans un dispositif de citation directe à comparaître, sans enquête menée par un·e juge d'instruction, avec une convocation au tribunal deux semaines après, ce qui laisse peu de marge de manœuvre pour se défendre. Les images de *sousveillances* qui arrivent dans les mains des avocat·es aident à disculper les victimes.

L'avocat Vincent Lurquin a ainsi raconté une affaire dans le cadre de laquelle de telles images se sont avérées extrêmement utiles. Une descente de policiers avait eu lieu à Beekkant (Molenbeek) pour des contrôles d'identité. Un jeune garçon était accusé d'avoir blessé un policier de manière grave ; il avait été arrêté et déféré devant un juge d'instruction. Entre-temps, ses amis avaient montré à l'avocat des vidéos qu'ils avaient prises ce jour-là : « *J'ai montré ça au juge qui a éclaté de rire car on voyait très bien que c'était le policier qui courait après les jeunes et que c'est le policier qui donnait des coups, genre kung-fu.* [...] *le jeune a pu sortir, il a été acquitté* [14]. »

Les images de *sousveillance* sont accessibles pour les avocats·es et elles jouent un rôle pour ouvrir une affaire ou pour faire entendre la parole de ces jeunes. La situation revêt cependant un caractère légèrement cynique car, de fait, ces vidéos semblent davantage permettre que des victimes de violences policières ne soient pas poursuivies, que d'amener à la condamnation des policier·es.

Systématiquement, pour se protéger, les policier·es portent plainte contre les personnes qu'ils frappent.

Il n'y avait pas d'images, et la version policière qui invoque la légitime défense face à un refus d'obtempérer, n'a pas pu être remise en cause.

2. Du côté de la société civile

Cependant, ces vidéos rendent visibles les violences policières et interpellent ceux et celles qui ne les vivent pas.

Juin 2023, Nanterre (en région parisienne), France. Nahel M., âgé de 17 ans, est tué d'une balle tirée à bout portant par un policier. Les policiers présents invoquent la légitime défense, affirmant que la voiture conduite par Nahel leur a foncé dessus. Mais une vidéo apparaît, révélant le mensonge policier : on y voit la voiture à l'arrêt, puis démarrant doucement dans le sens inverse des policiers, et l'un des policiers tirant à bout portant en direction du conducteur. La diffusion de ces images suscite l'indignation et la France s'embrase. Pendant plusieurs jours, la révolte jaillit dans plus de 300 villes françaises. La colère se propage en Belgique. Cette séquence remet sur le devant de la scène médiatique et politique les violences policières, et plus largement les violences et discriminations raciales et sociales que vivent les populations des quartiers populaires.

Les images sont au cœur de cet événement. Il y a la vidéo de la mort de Nahel. Cette image qui déconstruit le récit mensonger policier, et qui, dans un même mouvement, remet en question tous les récits policiers précédents qui invoquaient la légitime défense pour inverser les responsabilités. Au centre de la colère, il y a cette image, mais aussi toutes les images qui n'existent pas : « *Sans la vidéo, Nahel n'aurait été qu'une statistique* » peut-on lire un peu partout. Quinze jours avant, Alhoussein Camara, 19 ans, a été tué par la police à Angoulême dans des circonstances très similaires. Il n'y avait pas d'images, et la version policière qui invoque la légitime défense face à un refus d'obtempérer, n'a pas pu être remise en cause.

Il y ensuite les images des révoltes qui circulent sur les réseaux sociaux et qui effraient les politicien·nes au point d'amener le président Macron à « *appeler les grandes plateformes à retirer les "contenus les plus sensibles", tout en leur demandant de collaborer pour identifier ceux "qui utilisent ces réseaux sociaux pour appeler au désordre ou pour exacerber la violence"* » [15]. Les images font peur : elles sont des témoignages, mais aussi des appels, des images agissantes.

15 août 2020, Parvis de Saint-Gilles, Bruxelles, Belgique. Trois femmes sont harcelées par un homme. La police intervient et se concentre sur le non-port du masque par les femmes. Elles sont arrêtées et brutalement violentées : lésions au cou, contusion à l'épaule, poignet cassé. Sur le moment, la commissaire commente : « *En même temps, avec des tenues comme ça, il ne faut pas s'étonner.* » Par la suite, dans la presse, la police a signalé que les trois victimes étaient en « *tenue légère* ».

Des témoins ont filmé la scène, l'un s'est vu saisir son téléphone, l'autre a été poursuivi jusqu'à chez lui, embarqué au commissariat où les policiers lui ont écrasé les parties génitales pour le forcer à effacer les vidéos [16]. Une vidéo de l'arrestation des femmes a quand même réussi à circuler sur les réseaux sociaux. Elle a été complétée par leur témoignage et ceux des filmeurs maltraités. L'arrestation violente des femmes et son traitement sexiste ont suscité l'indignation. Une manifestation pour la dissolution de la brigade incriminée, la brigade UNEUS [17], s'est déroulée quelques jours après. Elle a marqué le début d'une convergence des luttes, notamment entre des groupes féministes et le collectif des Madrés, qui, depuis 2018 combat les violences policières que subissent les jeunes à Saint-Gilles [18]. La mobilisation a pris de l'ampleur, et cette lutte locale s'est avérée victorieuse avec la dissolution de la brigade UNEUS en 2022.

La mobilisation a pris de l'ampleur, et cette lutte locale s'est avérée victorieuse avec la dissolution de la brigade UNEUS en 2022.

S'il s'agit clairement d'une séquence où le contre-pouvoir a été effectif, le rôle des vidéos est difficilement mesurable. Elles ont probablement aidé à visibiliser les violences que subissaient au quotidien une partie de la jeunesse du quartier et à sensibiliser des habitant·es. Le rapport de force s'est inversé, et alors que le collectif des Madrés étaient raillé par le bourgmestre Charles Picqué lors de leur première interpellation au conseil communal en 2018, en 2020 celui-ci dû être suspendu face à la pression collective. Encore une fois, ce rapport de force se ressent dans l'expression de la peur du côté des politiques : à la suite de la diffusion des images de l'arrestation musclée des femmes, Charles Picqué déclare : « *La police n'a toujours pas compris que la bataille de la communication s'engage aussi sur les réseaux sociaux.* [...] *On doit être à égalité sur le plan des témoignages par l'image.* » L'année d'après, il débloque un budget colossal pour développer l'usage des bodycams dans la commune.

Le meurtre de Nahel ou l'arrestation de ces femmes à Bruxelles : les faits, leurs impacts, les pays et les contextes politiques ne sont pas les mêmes. Ces événements et ces images ne sont pas cités pour être comparés, mais ce sont des exemples où un événement, sa captation et la diffusion des vidéos ont provoqué quelque chose. Ces images interpellent et, parfois, permettent des mobilisations. Ces mobilisations peuvent prendre la forme de révoltes urbaines, de manifestations, d'interpellations communales ou de soutien aux procédures judiciaires.

Pour autant, certaines limites quant au rôle et à l'impact des images de *sousveillances* sont à souligner :

- Un déséquilibre des forces demeure : les images sont du côté de ceux et celles qui ont le pouvoir, notamment celui d'empêcher l'autre camp de filmer (par un arsenal législatif, par l'intimidation, ou par l'usage de la force). Filmer est alors une prise de risque, surtout pour les personnes racisées qui sont déjà la cible des policier·es.
- Les images de violences policières montrent des corps racisés frappés, mutilés, tués, au risque « *d'alimenter les stéréotypes d'une violence spécifique liée à la destinée noire* » [19], et au risque aussi de déclencher chez les personnes racisées qui voient ces images un « *trauma racial* » [20]. Ces images sont un outil du débat public, mais avoir conscience de leur violence et de leur inscription historique permet à toute personne qui entreprendrait de les diffuser de se poser la question de la pertinence d'une telle démarche, d'avoir un regard critique sur nos pulsions voyeuristes, et de prendre la précaution de les accompagner d'une mise en garde pour laisser le choix de leur visionnage ou non.
- « *Combien de Nahel n'ont pas été filmés ?* » Cette question doit rester centrale afin que les rares images de violences policières qui nous parviennent ne fassent pas contre-emploi en invisibilisant toutes les autres violences qui ne sont pas filmées.

RENDRE VISIBLE

Il semblerait que la police soit majoritairement perçue à travers le prisme de sa mission première : protéger. Il est alors difficile d'imaginer, pour beaucoup de personnes, que cette mission soit souvent dévoyée, au point que la police soit dangereuse pour une partie de la population. Il est alors nécessaire de proposer un contrepoint aux récits dominants. Les images, lorsqu'elles ne sont pas produites par la police, peuvent aider à rendre visibles les violences policières : cela permet alors une maîtrise de la production d'images, du point de vue adopté, et de leur chaîne de diffusion. Cependant, les images ne se suffissent pas à elles-mêmes : elles doivent être resignifiées, notamment pour apporter une lecture qui prenne en compte les rapports classistes et racistes qui sont à l'œuvre, aussi bien dans la dynamique systémique des violences policières que dans le traitement des images de ces dernières.

Les images de *sousveillances* sont alors centrales pour appuyer les contre-récits qui dénoncent ces violences sur les réseaux sociaux, dans des contre-enquêtes journalistiques, dans des expertises scientifiques ou judiciaires. L'impact de ces contre-récits semble cependant davantage se situer au niveau de la sensibilisation de la société civile et de sa mobilisation, que du côté des procédures judiciaires et inculpations de policier·es incriminé·es. Mais la coexistence des différentes formes de contre-pouvoir se nourrissent souvent mutuellement. ❏

« Combien de Nahel n'ont pas été filmés ? »

FILMER LA POLICE EST UN DROIT

➡ Filmer la police n'est pas interdit et dans le droit belge, ce qui n'est pas interdit est autorisé.
➡ Filmer la police est reconnu par la jurisprudence comme un usage de contrôle démocratique.
➡ Le droit à la vie privée du ou de la policier·e doit s'effacer si l'intérêt de la liberté d'expression ou du droit à l'information des citoyen·es est supérieur (art. 10 CEDH ; art. 25 Constitution).
➡ La police n'a pas le droit de saisir un téléphone ou d'obliger à effacer des images.
➡ Si les images ont un lien avec une infraction, la police a le droit d'obtenir les images, mais uniquement dans le cadre d'une procédure de « saisie judiciaire » (en suivant la procédure judiciaire).

La diffusion des images peut être source de litige et est soumise à une réglementation.
➡ On a toujours le droit de communiquer les images à la presse ou aux autorités judiciaires.
➡ Si les policier·es ne sont pas reconnaissables, on a toujours le droit de diffuser les images.
➡ Si les policier·es sont reconnaissables, on a le droit de diffuser les images sans l'autorisation de la personne concernée si :
- l'objectif est de contribuer au débat public d'intérêt général,
- en exerçant notre droit journalistique d'informer, l'expression universitaire, artistique ou littéraire,
- en exerçant notre liberté d'expression : ce droit comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations.

Le droit à la vie privée des policier·es et la liberté d'expression peuvent alors être en contradiction. Seul·e un·e juge pourra trancher.

L'application du droit est à géométrie variable.
Ibrahima Barrie est mort en cellule après avoir été arrêté alors qu'il filmait une intervention de police sur un groupe de personnes migrantes à la gare du Nord.
De nombreuses personnes voient leurs téléphones confisqués, sont arrêtées, frappées ou tuées, parce qu'elles filment. Le contrôle d'identité pour arrêter une personne en train de filmer sert souvent de prétexte légal. Encore une fois, les jeunes personnes racisées sont davantage victimes de ces abus. C'est pourquoi, les images ont beau être utiles, cela peut être nécessaire d'être prudent·e pendant la prise de vue (ne pas être en situation d'outrage, rester discret·e, enregistrer directement en ligne avec Snapchat par exemple, etc.).

Sources : Mathieu Beys, *Quels droits face à la police ?*, Couleur livre, 2014 et Caroline Carpentier, avocate.
Voir aussi : https://policewatch.be/files/filmer_la_police_le_livret.pdf & https://obspol.be/vos-droits/

1. Ce texte est une synthèse de l'article « La guerre des récits » publié sur le site www.surveillances.be
2. Universitaire canadien, considéré comme le père de la technologie portable, il vit avec une caméra solidaire de son crane.
3. A. GUNTHERT, « Filmer la police contrarie le maintien de l'ordre », blog *L'image sociale*, novembre 2012.
4. D. DUFRESNE, *Police*, éd. La Fabrique, 2020.
5. E. LEMAIRE, *L'œil sécuritaire. Mythes et réalités de la vidéosurveillance*, La Découverte, 2019.
6. *Le Monde*, 30 juin 2023.
7. https://forensic-architecture.org/
8. https://www.index.ngo/
9. https://www.retrace.be/
10. Lire « Vidéosurveillance et violence policière : un champ obstrué », p. 7-9.
11. Rapport d'analyse sur les bodycams de Police Watch (LDH), 2022.
12. Entretien réalisé le 8 février 2022.
13. Entretien réalisé le 10 mars 2022. Voir à ce propos l'arrêt Boutaffala : la Cour européenne des droits de l'homme a condamné la Belgique pour violation de l'art. 6 de la Convention européenne des droits de l'homme protégeant le droit au procès équitable.
14. Entretien réalisé le 9 juin 2023.
15. *Le Monde*, ibid.
16. P. CISELET, « - de keufs + de meufs : des féministes contre les violences policières à Saint-Gilles », *Bruxelles en mouvements* n°310, 2021.
17. La brigade UNEUS (Union pour un environnement urbain sécurisé) a été créée à l'initiative de la commune de Saint-Gilles en 2012.
18. https://www.collectifdesmadres.be/
19. A. GUNTHERT reprend l'analyse de la chercheuse M. PRICE dans « George Floyd : les images de violence imposent-elles la vision des bourreaux ? », blog *L'image sociale*, 12 juin 2020.
20. E. DEPRIS « Trauma Racial : l'impact du racisme sur la santé mentale », *BePax*, 21 décembre 2020.v

PETIT PAYS, BIG DATA

LE DÉVELOPPEMENT DE LA POLICE « PRÉDICTIVE » EN BELGIQUE [1]

Ces dernières années, la police dite « prédictive » [2] s'est imposée comme un vecteur de transformation au sein des services de police à travers le monde, remodelant le paysage de la prévention et de la répression. Cette approche promet d'améliorer l'efficacité de la police en misant sur les algorithmes et les bases de données, marquant apparemment le début d'une nouvelle ère pour le maintien de l'ordre. Qu'en est-il en Belgique ?

Corentin Debailleul[3], IGEAT-ULB

La police « prédictive » est une approche du maintien de l'ordre qui s'appuie sur l'analyse des données et les algorithmes « d'apprentissage automatique » (*machine learning*) pour « prédire » et ensuite chercher à « prévenir » les potentielles activités criminelles. On utilise les données historiques de la criminalité, ainsi que divers autres facteurs sociodémographiques et environnementaux, pour identifier des modèles et des tendances qui suggèrent où et quand, ou par qui, un crime est le plus susceptible de se produire. Les principaux objectifs de la police « prédictive » sont d'allouer les ressources policières de manière plus efficace en anticipant et en devançant l'activité criminelle dans certains lieux, ou en « prédisant » quels individus seraient des criminel·les potentiel·les afin de les surveiller de plus près, voire de justifier des interventions policières telles que des contrôles d'identité, des fouilles, voire des arrestations.

Or, l'utilisation d'algorithmes dans le domaine de la police est préoccupante à plus d'un titre : les biais algorithmiques renfoçant les discriminations – on y reviendra – mais aussi la difficulté (voire l'impossibilité) de rendre compte de manière transparente des décisions prises, que ce soit pour des raisons de sécurité, de secret d'industrie ou parce que les procédés utilisés sont issus de mécanismes « d'apprentissage automatique », par nature inintelligibles.

En Belgique, pour la Ministre de l'Intérieur Annelies Verlinden, l'avenir de la police sera numérique, et c'est le projet *i-Police* de la Police Fédérale qui devra faire entrer le Royaume dans le XXIe siècle.

UNE CRIMINOLOGIE SUSPECTE

Mais avant de plonger dans le programme fédéral, intéressons-nous aux quelques initiatives développées au niveau local, en particulier dans les zones de police *Westkust* (La Panne, Coxyde et Nieuport), *Zennevallei* (Beersel, Hal et Leeuw-Saint-Pierre) ou encore Anvers [4]. Celles-ci développent des mesures basées sur la *cartographie de « zones à risque »* potentiellement plus exposées aux activités criminelles. Au fondement de cette méthode, on retrouve une hyptohèse criminologique qui suppose que certaines zones géographiques attirent ou génèrent intrinsèquement des activités criminelles [5].

Or, cette hypothèse n'est pas étayée par des données empiriques, dans la mesure où les causes de la criminalité sont plutôt à chercher dans une interaction complexe entre divers facteurs sociaux, économiques et individuels. En mettant l'accent sur la dimension « environnementale », on néglige les facteurs socio-économiques et structurels sous-jacents de la criminalité. En outre, l'accent mis par ces cartographies sur les facteurs environnementaux peut involontairement renforcer les préjugés en ciblant de manière disproportionnée certains quartiers sur la base des données de criminalité passées. Cela peut perpétuer des pratiques déjà à l'œuvre, ciblant les quartiers défavorisés et exacerbant les inégalités existantes. Comme l'explique le géographe Brian Jefferson :

> *« La manière dont les préjugés de la police et de la Justice affectent les statistiques de criminalité n'est pas systématiquement explorée par ces approches. Elles n'abordent pas non plus la façon dont les lois, les politiques ou les pratiques policières influencent les motifs géographiques dessinés par les données de criminalité. Les cartes de criminalité n'offrent pas tant des images définitives et objectives des comportements illégaux, mais soulèvent plutôt des questions sur la manière dont ces comportements sont enregistrés et étudiés* [6]. »

Cela n'empêche pas certain·es criminologues d'en faire une carrière. En 2023, un professeur de l'Université de Gand s'est vu attribuer près de 2 millions d'euros par l'Union Européenne pour mener à bien un projet nommé BIGDATPOL [7]. L'objectif de la recherche est d'intégrer les aspects statistiques, criminologiques, économiques, juridiques et éthiques dans un modèle fournissant « *à la fois aux mondes académique et policier des lignes directrices et des recommandations pour étudier, appliquer et mettre en œuvre le maintien de l'ordre fondé sur les big data* » [8].

> En mettant l'accent sur la dimension « environnementale », on néglige les facteurs socio-économiques et structurels sous-jacentes de la criminalité.

En Belgique, pour la Ministre de l'Intérieur Annelies Verlinden, l'avenir de la police sera numérique, et c'est le projet *i-Police* de la Police Fédérale qui devra faire entrer le Royaume dans le XXIe siècle.

GARBAGE IN, GARBAGE OUT

« *Un "pop-up" apparait* [...] *afin de signaler qu'une "anomalie", donc quelque chose d'inhabituel, a été constatée. L'application policière a enregistré un nombre élevé de vols de bicyclettes autour d'un certain endroit et à certains moments. Le système peut détecter cela parce que nos "data scientists" à Bruxelles ont programmé le système pour reconnaître des "anomalies" de ce type.* [...] *Le système indique que certains agissements suspects ont été récemment signalés à cet endroit.* [La commissaire] *prévoit une patrouille récurrente* [9]. »

On pourrait croire à un début de livre de mauvaise science-fiction, mais il s'agit d'un extrait de l'appel d'offre publié par la Police Fédérale pour le lancement de son projet i-Police, un programme fédéral doté depuis 2021 d'un budget de 300 millions d'euros. Il vise à interconnecter différentes bases de données (locales et fédérales ; belges et européennes ; internes et externes) et à refonder l'architecture informatique de la police en y incorporant des logiciels d'analyse et de prédiction.

L'ambition n'est pas des moindres, selon le commissaire général de la Police Fédérale : « i-Police *fera de la police belge l'une des forces de police les plus avancées d'Europe en termes de gouvernance des données. Le système analysera les informations, les mettra automatiquement à la disposition des forces de police, fera des propositions d'enquête et fournira de nombreux outils pour gagner du temps, comme les traductions automatiques. i-Police nous permet de frayer le chemin pour une Police Intégrée orientée vers l'avenir, au service des citoyens* [10]. »

Cependant, le programme i-Police suscite quelques préoccupations, notamment parce qu'il concerne l'utilisation d'algorithmes opaques et la centralisation de grandes quantités de données au sein d'un système unique. i-Police prévoit en effet de rassembler la Banque de données nationale générale (BNG) et ses millions d'entrées [11], des bases de données locales dont la légitimité est souvent discutable [12], les bases de données communes rassemblant « terroristes » et « propagandistes de haine » et d'autres sources internes et externes à la police. i-Police est donc appelé à rassembler quantité d'informations parmi lesquelles il sera difficile (voire impossible) de distinguer lesquelles ont été vérifiées, et lesquelles relèvent de rumeurs ou de suppositions.

Les systèmes de police « prédictive » s'appuient en premier lieu sur les bases de données policières. Cependant, celles-ci rendent difficile toute contestation réelle en raison de l'absence de droits d'accès direct et de voies de recours significatives [13]. Pourtant, ces bases de données peuvent avoir de sérieuses répercussions sur les personnes, dans la mesure où les inexactitudes et les classifications injustes peuvent entraîner des fouilles injustifiées ou des contrôles de sécurité renforcés (notamment dans les aéroports). Des informations fallacieuses peuvent porter atteinte à la réputation et aux moyens de subsistance d'une personne dont l'emploi peut être menacé.

Des données d'entrée peu fiables ne peuvent pas, comme par magie, produire des résultats de qualité.

Plusieurs rapports soulignent les manquements de la police belge en matière de gestion des bases de données et de respect des droits fondamentaux [14]. La police a en particulier été pointée du doigt pour ses pratiques de profilage ethnique [15] et pour son usage répété de logiciels de reconnaissance faciale, hors de tout cadre légal [16]. En outre, la surveillance policière en général et notamment des travailleuses du sexe ; des « bandes » urbaines ; ainsi que des personnes dites « radicalisées », ciblent de manière disproportionnée les groupes déjà marginalisés et renforcent les inégalités existantes. Sans contre-mesures sérieuses, l'automatisation du maintien de l'ordre ne pourra qu'exacerber ces problèmes. ➡

DE SULFUREUX SOUS-TRAITANTS

Il est difficile de déterminer avec précision quelles entreprises et logiciels seront intégrés dans le programme i-Police. Ce qui est clair, c'est que la société française d'informatique et de conseil Sopra Steria assume le rôle de maître d'ouvrage, avec le soutien de la société de conseil KPMG. Selon un article de presse, elles collaboreront avec un large éventail de sous-traitants, dont des sociétés telles que Microsoft, la société canadienne Niche et les sociétés israéliennes Interionet et TA9/Rayzone [1].

Selon une source anonyme, l'implication d'une société dans des scandales internationaux a entraîné son exclusion en tant que fournisseur potentiel de logiciels pour i-Police. Toutefois, cette société inconnue n'est pas la seule à susciter des inquiétudes. Par exemple, le sous-traitant d'i-Police Interionet est dirigé par Yair Pecht, l'ancien directeur général du groupe israélien NSO, spécialiste de la cyberoffensive. NSO est la société tristement célèbre pour avoir produit le logiciel espion Pegasus. Les antécédents controversés de NSO, marqués par des transactions avec des régimes autoritaires, ont attiré l'attention de la communauté internationale, ce qui a conduit ses dirigeants à multiplier le nombre de start-ups satellites, telles qu'Interionet [3].

Malgré cette tentative de se refaire une virginité, Interionet fait l'objet d'une campagne de boycott. Le mouvement BDS, qui milite pour le respect du droit international en Israël/Palestine, appelle les Belges à s'opposer au contrat entre la Police Fédérale et Interionet en raison de l'expérimentation de son logiciel de surveillance sur les Palestinien·nes avant sa commercialisation à l'échelle mondiale [3]. Une telle pratique n'est pas rare, comme le révèle un livre récent du journaliste Antony Loewenstein : « le complexe militaro-industriel israélien utilise les territoires palestiniens occupés comme terrain d'essai pour l'armement et les technologies de surveillance qu'il exporte ensuite dans le monde entier à des démocraties comme à des despotes [4]. »

1. L. BOVÉ et J.-P. BOMBAERTS, « La police entame une révolution digitale à 300 millions d'euros », *L'Echo*, 7 mai 2022.
2. B. PETERSON, « The founders of a billion-dollar Israeli spyware startup accused of helping Saudi Arabia attack dissidents are funding a web of new companies that hack into smart speakers, routers, and other devices », *Business Insider*, 9 mai 2019.
3. BDS Movement, « Don't let the Belgian police use Israeli apartheid surveillance against Belgians! », Facebook [@BDSNationalCommittee].
4. A. LOEWENSTEIN, *The Palestine laboratory: How Israel Exports the Technology of Occupation Around the World*, Verso Books, 2023.

En informatique, le principe *garbage in, garbage out* indique que des données d'entrée peu fiables ne peuvent pas, comme par magie, produire des résultats de qualité. C'est précisément ce que l'on peut craindre avec le développement de la police « prédictive » en Belgique : à l'entrée des bases de données teintées de préjugés racistes et à la sortie des contrôles au faciès 2.0.

PRÉVISIONS HOULEUSES

Trois ans après le lancement du marché public i-Police, la mise en place d'un système d'échange de données au niveau international a démarré et une phase pilote du projet a été lancée à Liège [17]. Lentement, mais pas si sûrement… le projet i-Police semble avoir eu du mal à démarrer. Un audit réalisé par Deloitte au sein de la direction informatique de la Police Fédérale conclut que la transformation numérique de la police n'a pas été bien pensée, ce qui entraîne une approche fragmentée, et que le contrôle interne est inadéquat quant à la façon dont le personnel policier utilise les bases de données, ce qui est susceptible de conduire à des abus [18]. Devant le Parlement Fédéral, les auteurs de l'audit ont déclaré :

« *Tout d'abord, pour les standards et la législation, nous avons constaté qu'il n'y a pas vraiment de gestion formalisée concernant l'exploitation opérationnelle des données, la sécurité, la protection des données. Nous avons constaté qu'il n'y a pas vraiment de stratégie non plus sur la sécurité de l'information* […]. *Nous avons constaté que le contrôle de gestion interne est limité, insuffisant dans le cadre de la gestion des informations* [19]. »

Par ailleurs, la Police Fédérale ne peut plus payer ses factures et le montant total des impayés s'élève à plusieurs dizaines de millions d'euros [20]. Selon un représentant syndical avec lequel nous nous sommes entretenus, le projet i-Police fait actuellement l'objet de sérieuses révisions visant à donner la priorité à la stabilité des opérations informatiques fondamentales de la police, réduisant considérablement les aspirations initiales du projet.

Tout cela soulève des questions sur la fonction des entreprises privées offrant des services de consultance à une Police Fédérale endettée. Et quels services ? Le développement d'i-Police a été attribué à un consortium Sopra Steria/KPMG pour ensuite confier à Deloitte le soin d'auditer le processus, et finalement conclure à un déficit de stratégie interne… Avec un peu de malice, on est en droit de se demander quelle société de consultance sera mandatée pour pallier cette carence.

Difficile finalement de s'y retrouver… Faut-il croire la police lorsqu'elle affirme utiliser des systèmes de haute technologie capables de traiter des données massives en vue de désigner les criminel·les potentiel·les ? Ou devons-nous nous ranger du côté de la conclusion de Deloitte selon laquelle l'organisation de la police laisse largement à désirer ?

Lors d'un entretien avec le directeur de l'Organe de contrôle de l'information policière, ce dernier a déclaré à propos de i-Police : « *Il y a une grande différence entre ce que dit la presse et la réalité. La police n'est pas du tout aussi performante qu'on le pense.* […] *Il y a un fossé énorme entre la communication et la situation sur le terrain* [21]. » Il est rassurant de savoir que le niveau de sophistication technologique de la police n'est peut-être pas à la hauteur de ce qu'elle proclame. Néanmoins, le développement d'i-Police devra être suivi de près. Il sera primordial de s'assurer qu'en cas d'abandon du projet, certains de ses aspects les plus problématiques ne seront pas recyclés sous un autre nom.

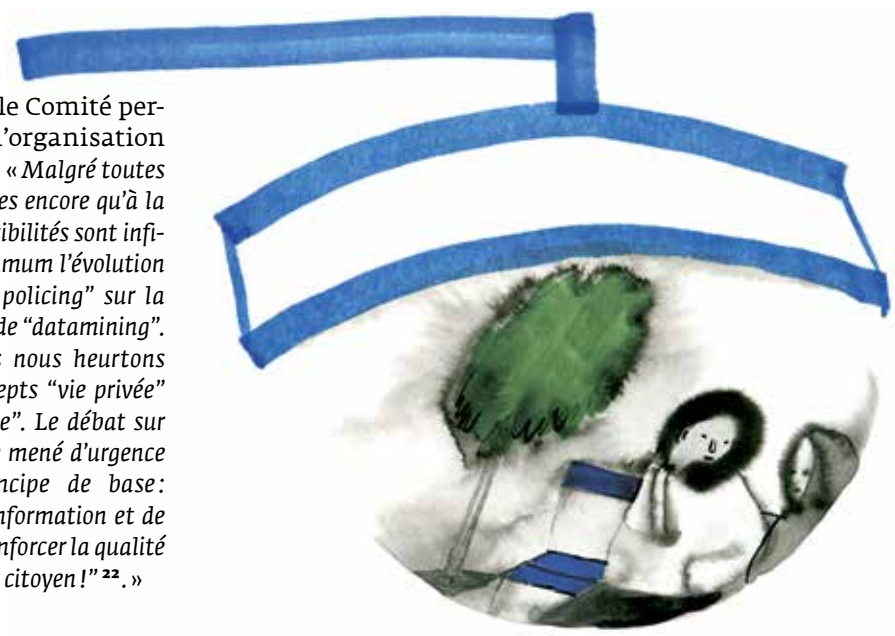
QUI PEUT PRÉDIRE L'AVENIR DE LA POLICE PRÉDICTIVE ?

Dans son document Horizon 2025, le Comité permanent de la police locale (CPPL), l'organisation coupole des zones de police, écrit : « *Malgré toutes les transformations* […], *nous n'en sommes encore qu'à la veille de ladite révolution. Les futures possibilités sont infinies avec comme summum l'évolution vers une "predictive policing" sur la base de "big data" et de "datamining". Tous les jours, nous nous heurtons aux limites des concepts "vie privée" et "droits de l'homme". Le débat sur la vie privée doit être mené d'urgence en ayant pour principe de base : "L'Exploitation de l'information et de la technologie pour renforcer la qualité de vie et la sécurité du citoyen !"* [22]. »

Tout cela soulève des questions sur la fonction des entreprises privées offrant des services de consultance à une Police Fédérale endettée.

Voilà qui trace clairement une ligne de front. La numérisation des pouvoirs publics est en marche, et la police ne fait pas exception. Partout, on entend parler de villes « intelligentes », de solutions « data-centrées », alors pourquoi pas de « smart policing » ? En attendant, on ne peut que constater d'importants manquements quant à la protection des données, à la transparence des algorithmes et aux impératifs de non-discrimination. Cependant, les associations de terrain comme les autorités de protection de données peinent à assurer un réel contre-pouvoir. Un réveil semble nécessaire pour que la liberté ne soit pas une nouvelle fois sacrifiée sur l'autel de l'innovation technologique. ❏

Un réveil semble nécessaire pour que la liberté ne soit pas une nouvelle fois sacrifiée sur l'autel de l'innovation technologique.



1. Cet article est issu d'une enquête commanditée par l'ONG Fair Trials et menée en parallèle en France, en Allemagne, en Espagne et au Royaume-Uni. Pour la France, voir « La Police prédictive en France : contre l'opacité et les discriminations, la nécessité d'une interdiction » sur www.laquadrature.net /
2. L'utilisation de guillemets autour du terme « prédictif » vise à rappeler que la police n'est pas réellement en mesure de prévoir les crimes futurs. La police dite « prédictive » est basée sur des algorithmes et des modèles statistiques qui fournissent des probabilités et non des prédictions fiables. Quoi qu'en disent les technoévangélistes, les visions prophétiques dignes de *Minority Report* appartiennent encore et toujours au domaine de la fiction.
3. Merci à Griff Ferris, Sofia Lyall, Emmanuelle de Buisseret Hardy et Sarah De Laet pour leurs contributions à cet article ou à la recherche sur laquelle il se base.
4. La police belge est structurée en deux niveaux : d'une part, la police fédérale, qui couvre tout le territoire belge et d'autre part 183 zones de police disposant localement d'une grande autonomie et rendant par là même extrêmement difficile de recenser toutes les initiatives prises localement.
5. H. B. SCHRAEDER et L. W. KENNEDY, « Risk Terrain Modeling (RTM) » in *The Encyclopedia of Research Methods in Criminology and Criminal Justice*, dir. J.C. Barnes & D. R. Forde, éd. Wiley, 2021, p. 873–874.
6. B. JEFFERSON, « Crime Mapping », in *International Encyclopedia of Human Geography*, éd. Elsevier, 2020, p. 11-15.
7. « Towards an evidence-based model for big data policing: Evaluating the statistical-methodological, criminological and legal and ethical conditions », résultats de recherche Cordis UE, 2023.
8. « Six Ghent University researchers win ERC Consolidation Grant », UGent, 31 mars 2023.
9. Annexe H de la description du marché i-Police, p. 35
10. Annelies Verlinden, « i-Police: l'avenir de la police est numérique », 7 mai 2022 [verlinden.belgium.be].
11. O. BAILLY, 'BNG, la base non gérée', *Médor*, 14 avril 2021.
12. D'après le COC : « *Lorsque nous effectuons des audits proactifs, nous demandons toujours de nous fournir une liste des bases de données particulières et d'expliquer pourquoi il est nécessaire de disposer de ces bases. Dans 99 % des cas, la moitié d'entre elles ont disparu lorsque notre enquête est terminée.* » Entretien du 17 février 2023.
13. C. FORGET, « L'effacement des données policières et judiciaires : un parcours du combattant ? », *e-legal*, vol. 6, 2022.
14. COC, « Rapport concernant les infractions commises par des membres de la police intégrée dans le cadre de traitements dans la BNG », Organe de contrôle de l'information policière, 2023, DIO23001 ; Voir aussi les rapports d'activité annuels du COC.
15. I. SAUDELLI, *Mag ik uw identiteitskaart zien? Een kwalitatief onderzoek naar identiteitscontroles uitgevoerd door de Belgische lokale politie*, Thèse de doctorat, Bruxelles, Vrije Universiteit Brussel, 2021.
16. Voir p.ex. le rapport d'activité 2022 ou les rapports DIO19005 ; DIO21006 ; DIO23001 de l'Organe de contrôle de l'information policière [www.organedecontrole.be].
17. Réponse de la Ministre Verlinden à la question 1964 de Daniel Senesael, député socialiste au Parlement Fédéral, 31/08/2023.
18. S. ROMANS. « Audit kraakt digitale transformatie van politie », *De Tijd*, 31 mai 2023.
19. Audit de la Direction de l'information policière et des moyens ICT de la Police Fédérale – Audition, Chambre des représentants de Belgique, Doc 55 3516/001.
20. X. COUNASSE, « La police fédérale ne peut plus payer ses factures », *Le Soir*, 16 août 2023.
21. Deuxième entretien avec l'Organe de contrôle de l'information policière, 11 octobre 2023.
22. Commission Permanente de la Police Locale (CPPL), Horizon 2025, 2019, p. 13.

QUAND LA TECHNOLOGIE S'EMPARE DE LA CONVERSATION

Depuis que l'informatique accompagne nos communications, il devient tentant pour les uns de nous envahir de publicités, pour d'autres d'examiner nos comportements. De telles tendances peuvent être au mieux désagréables, au pire de vrais dangers pour la démocratie. Cet article retrace l'historique des conversations numériques, dénonce certains travers et formule quelques principes fondamentaux à défendre pour que la surveillance généralisée de nos correspondances reste dans les livres de science-fiction.

Benoît Coumont, IEB

Il y a près de 60 ans, le courrier électronique naissait, dans le sillage des premiers ordinateurs et d'Internet, d'une collaboration entre universitaires s'appuyant sur des travaux menés par l'armée états-unienne. Apparu à une époque où le concept de brevet logiciel n'existait pas, la technologie derrière cet outil de communication a peu évolué et est, depuis le début, largement documentée. Cette absence de propriété a rendu inutile la création de protocoles alternatifs qui n'auraient pas forcément été interopérables. Il aurait fallu, lors de la rédaction d'un e-mail, s'assurer que son correspondant utilise une technologie compatible. L'e-mail n'aurait alors certainement pas connu le succès et l'utilisation massive qu'il connaît encore aujourd'hui.

IL ÉTAIT UNE FOIS…

La situation est tout autre pour les outils de communication qui ont suivi. Le SMS a été introduit avec la norme GSM, technologie qui s'est imposée dès les années 1990. Le contexte est différent : les commerciaux sont cette fois à la manœuvre et le finlandais Nokia est le grand gagnant de cette bataille industrielle qui a su imposer ses normes au monde entier. La technologie est ouverte[1], mais les opérateurs de télécommunications facturent des coûts additionnels pour passer d'un réseau à l'autre.

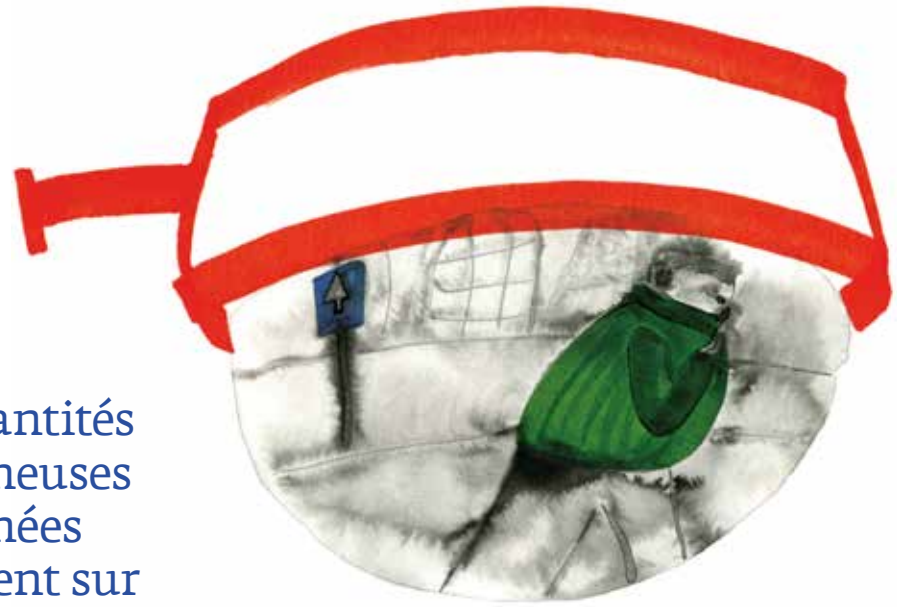
Ces coûts – qui seraient bien moins élevés, si du regretté Belgacom, nous avions au moins conservé dans le giron public la maintenance du réseau, limitant ainsi fortement les conséquences environnementales, sanitaires et économiques liées à la multiplication des réseaux 2G, 3G, 4G, 5G et fibre optique[2] – sont avec certaines limitations techniques la raison du déclin progressif du SMS au profit des messageries instantanées.

> Avec le logiciel ICQ en 1996, la société israélienne Mirabilis apporte des fonctionnalités au tchat que l'on appelle dès lors, messagerie instantanée.

En 1988, le protocole standard ouvert Internet Relay Chat (IRC) naît dans un contexte universitaire similaire à celui de la création de l'e-mail pour permettre l'échange de messages en temps réel. Il faudra cependant attendre la fin des années 1990 et la démocratisation d'Internet pour que le *salon de conversation* s'ouvre aux non-ingénieur·es avec Caramail, premier succès commercial du genre en Europe francophone. Mais bien que l'outil repose, en grande partie, sur des technologies ouvertes et libres de droit, Caramail et ses concurrents en feront des réseaux fermés et non-interopérables – et ce, pour des raisons purement commerciales et non techniques.

Avec le logiciel ICQ en 1996, la société israélienne Mirabilis apporte des fonctionnalités au tchat que l'on appelle dès lors messagerie instantanée : authentification, gestion de contacts, etc. Les grandes entreprises du numérique proposent à leurs tours leurs solutions : AIM, Yahoo! Messenger, MSN Messenger, etc. Autant de réseaux propriétaires, fermés et incompatibles proposés gratuitement dans le but d'engranger un grand nombre de clients à qui proposer des services payants supplémentaires et de la publicité.

En parallèle naît le standard ouvert et normalisé XMPP (anciennement Jabber), alternative aux messageries instantanées commerciales. Dans l'esprit du logiciel libre, celui-ci ne contraint pas les choix des logiciels à utiliser, tant du côté serveur que du côté utilisateur. Google, Facebook, WhatsApp et bien d'autres s'appuieront sur cette technologie ouverte pour créer leurs services de messagerie. Presque tous ces grands acteurs s'en détourneront cependant pour développer leur propre solution après avoir construit de solides bases d'utilisateur·ices. Une fois encore et bien que XMPP soit conçu pour que les utilisateur·ices de différents fournisseurs de service communiquent entre eux, très peu des solutions commerciales activeront pourtant cette fonctionnalité. ➡



À L'ÈRE DES SMARTPHONES

Aujourd'hui, les messageries sont conçues pour le téléphone, devenu intelligent. Ainsi, WhatsApp, Telegram ou encore Signal se basent sur le numéro de téléphone comme identifiant et sur la présence d'une carte SIM associée en guise d'authentification. Ces applications réclament l'accès au carnet d'adresses pour y récupérer les autres utilisateur·ices du service. Cela pourrait être considéré comme une atteinte grave au respect de la vie privée, mais c'est paradoxalement aussi ce qui fait le succès de ces messageries : il n'y a plus de mot de passe et plus besoin de chercher des contacts. Si le numéro de téléphone d'un·e utilisateur·ice WhatsApp est inscrit dans le carnet d'adresse d'un·e autre, celui-ci sera joignable via WhatsApp – qu'on le veuille ou non. Pour forcer ce fonctionnement, WhatsApp rend obligatoire le téléchargement de son application officielle depuis un *AppStore* sur smartphone ; rendant les accès alternatifs (logiciels pour ordinateurs de bureau ou sites web dédiés) caduques ou limités.

Ces services atteignent alors des taux d'utilisation jamais égalés : 2 milliards d'utilisateur·trices pour WhatsApp [3], 1 milliard pour Google Messages [4] qui se base sur le succès de son système d'exploitation Android ou encore plus d'1 milliard pour Facebook Messenger [5].

L'évolution de ces services couplée à l'amélioration constante des débits de connexions ont rendu populaire l'utilisation de flux vidéos et audios faisant dès lors transiter des quantités vertigineuses de données sur des centaines de serveurs répartis dans le monde (occidental). Outre le coût environnemental conséquent [6], la gestion d'un tel service nécessite une infrastructure considérable. Par ailleurs, Meta (maison mère de Facebook et WhatsApp) et Google ne s'en cachent pas : leurs revenus sont presque exclusivement issus de la publicité. C'est que grâce au développement de l'intelligence artificielle, les données échangées sur ces services dressent des profils de plus en plus complets de ses utilisateur·ices – profils qui se vendent très cher auprès des agences publicitaires.

> Des quantités vertigineuses de données transitent sur des centaines de serveurs répartis dans le monde.

Mais aujourd'hui, la plupart de ces services annoncent intégrer le chiffrement des messages [7]. Autrement dit, il devient impossible pour toute personne extérieure à la conversation et même pour les fournisseurs de service de lire les messages échangés. Ces derniers détiennent cependant encore les métadonnées du message – soit l'identité des correspondant·es, leurs localisations, la date des échanges, etc. ainsi que, dans le cas de WhatsApp par exemple, des données transmises par le téléphone tel que le carnet d'adresse. Cela est loin d'être anodin [8] ! Tout en se targuant de respecter la vie privée, WhatsApp & cie continuent d'accumuler des données pour leurs partenaires publicitaires, vraisemblablement en quantité suffisante pour rentabiliser des services coûteux offerts « gratuitement » [9]. En Europe, le règlement général sur la protection des données (RGPD) nous protège partiellement, mais le non-respect et les contournements des lois sont nombreux [10].

Des services de messageries gratuites, on en compte des dizaines aujourd'hui. Ils ont presque tous des modèles économiques similaires basés sur l'exploitation des données. Trois d'entre eux se démarquent toutefois par une communication axée sur le respect de la vie privée et sont pour cela plébiscités aujourd'hui dans les milieux militants : **Telegram**, **Signal** et **Element**.

COMPARONS DONC

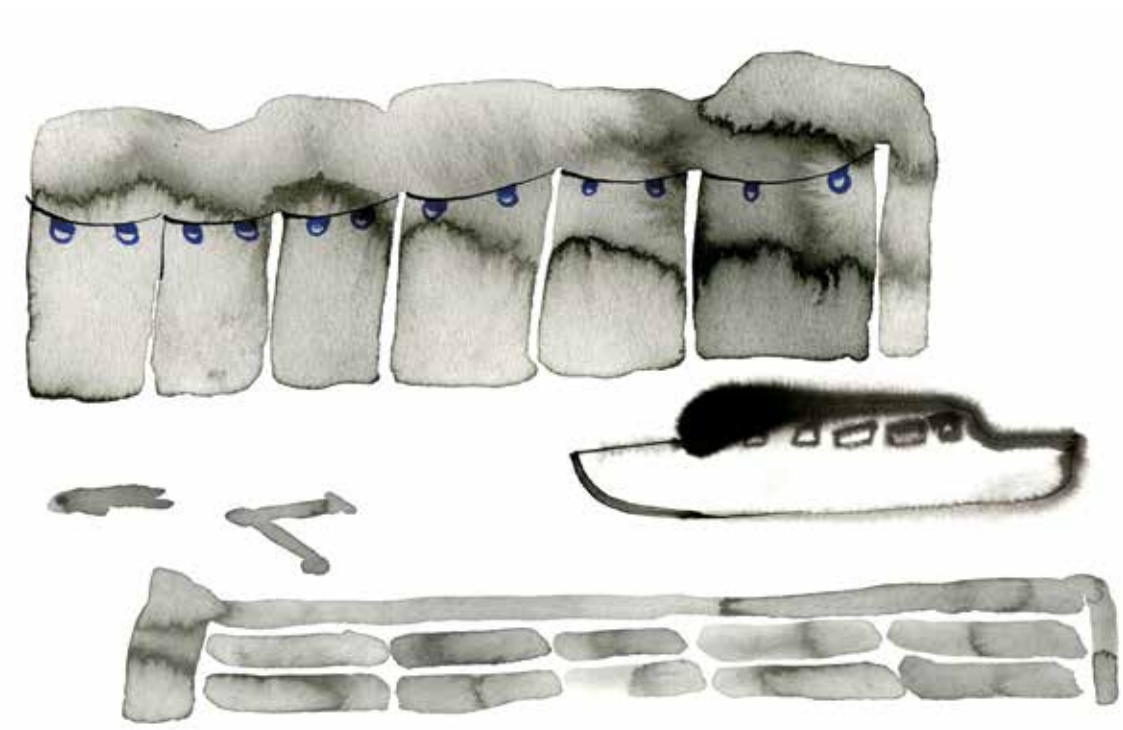
Méritent-ils cette confiance ? La réponse à cette question ne peut pas être objective. La promotion d'un outil au détriment d'autres est forcément subjective, en raison notamment des évolutions rapides dans ce domaine. Relevons, toutefois, certains points d'attention à observer dans le contexte d'une surveillance des communications appelée à croître.

1. Le financement. Offrir des correspondances écrites, audio et vidéo sans restrictions représente un coût qui peut se révéler vertigineux. Signal, revendiquant 40 millions d'utilisateur·ices en 2023, l'estime à 50 millions de dollars par an [11].

Selon ses dires, Signal se financerait exclusivement avec des dons et des subventions publiques. Parmi les dons, signalons 50 millions de dollars offerts par Brian Acton, co-fondateur de WhatsApp et désormais fâché contre Meta [12], et 1 million de dollars annuel offert par Jack Dorsey, co-fondateur de Twitter.

Telegram dépend d'un modèle économique bien plus classique (abonnements, publicités, etc.) avec le financement du milliardaire russe Pavel Dourov qui serait motivé par l'idée d'offrir un service échappant au FSB (service de renseignement russe).

Enfin, Element s'appuie sur un réseau associatif – comprenant **Domaine Public** à Bruxelles – pour proposer son service. Le développement logiciel est quant à lui assuré par sa principale contributrice, la société britannique Element, se finançant en proposant l'intégration de ses services aux collectivités [13].



> Ces applications réclament l'accès au carnet d'adresses pour y récupérer les autres utilisateur·ices du service.

2. L'ouverture des codes. La disponibilité du code source est un gage de transparence et de sécurité, offrant aux développeur·euses la possibilité d'étudier le logiciel et d'en proposer des modifications ou d'autres versions[14]. Iels corrigent les bugs plus vite et analysent le fonctionnement du logiciel pour certifier qu'il corresponde aux promesses de l'éditeur (sur l'absence de traqueurs par exemple). Distinguons ici deux types de logiciels utilisés par les services de messagerie : serveur et client. Le premier est installé par le fournisseur de service, le second correspond à ce que vous installez sur votre machine.

Cette distinction est importante car si les logiciels clients de Telegram, Signal et Element sont tous trois ouverts, il n'en est pas de même des logiciels serveurs. Celui de Telegram n'est pas libre, celui de Signal l'est partiellement et celui d'Element l'est entièrement.

Ainsi, l'ouverture des codes clients n'empêche pas Telegram et Signal d'empêcher ou de contraindre la création de logiciels clients alternatifs. Il est, par exemple, impossible de créer un compte Telegram sur un client non-officiel. Signal interdit, quant à lui, l'accès à ses serveurs de tout logiciel alternatif, tel **LibreSignal** qui en a fait les frais[15]. Element promeut la diversité des logiciels pouvant se connecter à son service. Il est d'ailleurs probable que vous en utilisiez un au quotidien : **Thunderbird**.

3. La décentralisation. La décentralisation du service répartit la charge entre plusieurs acteurs et serveurs offrant ainsi le choix entre plusieurs fournisseurs. Chacun pouvant disposer de ses propres conditions, de son éthique et de contraintes légales différentes. Seul Element répond à ce critère. Signal et Telegram invoquent la volonté de contrôler l'entièreté de la chaîne et de limiter les contraintes techniques et les coûts nécessaires à une telle intégration.

4. La gouvernance. À qui appartiennent ces services, logiciels et serveurs ? Et comment se prémunissent-ils d'un changement de propriété ?

Telegram est une entreprise aux mains de son PDG et fondateur Pavel Dourov. Elle pourrait être vendue et changer d'orientation selon les desiderata de son·sa propriétaire. Signal dépend d'une fondation qui ne pourrait théoriquement pas être rachetée et dont les valeurs seraient ainsi pérennes. Notons cependant que Brian Acton est présent dans plusieurs instances de décisions de Signal depuis son don de 2020[16]. Element est une société basée à Londres avec des filiales en France et en Allemagne. Elle pourrait être rachetée, mais la disponibilité totale du code source permettrait alors à d'autres acteurs de poursuivre la mission originelle.

5. L'anonymat. Le numéro de téléphone associé à l'appareil sert généralement de compte utilisateur. Comme il n'est plus possible d'acheter une carte SIM sans donner son identité, l'anonymat est illusoire dans ces conditions.

Or, Signal et Telegram requièrent tous deux un numéro de téléphone. Signal propose depuis peu de cacher le numéro à ses contacts, mais celui-ci est toujours bien nécessaire pour la création du compte. Element n'exige ni téléphone, ni même d'adresse e-mail.

6. Les métadonnées. Toute communication électronique s'accompagne de données annexes à la conversation (date, lieu, etc.)[17]. Signal semble être assez minimaliste à ce sujet. Telegram en envoie plus et Element en envoie beaucoup. Ce dernier avance, à ce sujet, des nécessités techniques dus à la décentralisation de son réseau.

En Europe, le règlement général sur la protection des données (RGPD) nous protège partiellement, mais le non-respect et les contournements des lois sont nombreux.

ET LE GAGNANT EST…

Element semble sortir vainqueur de cette comparaison. Mais comme mentionné au préalable, ces arguments sont subjectifs et d'autres critères pourraient changer la donne, tels que la popularité du service, la facilité de retrouver des contacts ou l'intégration à d'autres services.

Le plus important n'est peut-être pas de savoir qui répond le mieux aujourd'hui à ces critères, mais plutôt qui pourrait y répondre demain dans un contexte croissant et international de surveillance des communications[18]. Quand des applications ne sont pas bannies[19], elles sont de plus en plus mises sous pression de « modérer » les contenus jugés sensibles ou criminels. Mais une telle modération de contenus signifierait donner le pouvoir à des individus ou des algorithmes (dépendant quasi exclusivement de sociétés privées) de lire des messages privés et de déterminer ce qui serait illégal ou immoral. On peut facilement imaginer les travers orwelliens d'une telle situation. ❑

1. Les spécifications du protocole SMPP utilisé pour l'échange de SMS sont publiées depuis 1997 [https://smpp.org/].
2. L'Institut belge des services postaux et des télécommunications (IBPT) cartographie les différents réseaux [https://www.bipt-data.be/]. Bien que deux des quatre opérateurs (Proximus et Orange) aient annoncé une fusion de leurs réseaux d'antennes GSM, les doublons continuent d'exister.
3. https://blog.whatsapp.com, 12 décembre 2020.
4. https://blog.google, 30 novembre 2023.
5. https://techcrunch.com, 12 avril 2017.
6. En 2016, le numérique représentait déjà 2 % des émissions de gaz à effet de serre, autant que l'aviation civile [Novethic.fr, 19 mai 2016].
7. À l'instar de Whatsapp en 2016 ou Facebook Messenger en 2022.
8. Le média israélien de langue anglaise *+972 Magazine* révèle que l'armée israélienne utilise les métadonnées de Whatsapp pour localiser ses cibles, 03 avril 2024.
9. Par ailleurs, les modèles économiques évoluent et ne sont plus centrés exclusivement sur la publicité. WhatsApp, par exemple, propose désormais des services supplémentaires payants aux entreprises tels des chatbots.
10. « RGPD : Facebook écope d'une amende record de 1,2 Md », *Le Monde Informatique*, 22 mai 2023.
11. Coût annoncé dans son appel aux dons [Signal.org, 16 novembre 2023].
12. « Signal's Brian Acton talks about exploding growth, monetization and WhatsApp data-sharing outrage », Techcrunch.com, 12 janvier 2021.
13. Tels le Gouvernement français qui le propose depuis 2019 à plus de 400 000 fonctionnaires, deux États allemands qui en ont fait le système de communication de 500 000 étudiant·es ou encore l'armée allemande avec près de 200 000 militaires.
14. La Free Software Foundation définit ainsi le logiciel libre : https://www.gnu.org/philosophy/free-sw.fr.html
15. https://github.com/LibreSignal/LibreSignal/blob/master/README.md
16. Signal.org, 10 janvier 2022.
17. Que sont les métadonnées et pourquoi sont elles importantes ?, Surveillance Self-Defense, 12 mars 2019 [https://ssd.eff.org].
18. Lire « Règlement CSAR : la surveillance de nos communications se joue maintenant à Bruxelles », 18 septembre 2023 [https://www.laquadrature.net].
19. Au printemps 2024, la France a bloqué l'accès au réseau social TikTok en Kanaky-Nouvelle-Calédonie durant les révoltes du peuple Kanak. Voir « Une histoire qui bégaie », Survie.org, 4 juin 2024.

PETIT GUIDE DE RÉSISTANCE NUMÉRIQUE

Ou comment contrer l'intelligence de son téléphone intelligent…

Benoît Coumont, IEB

Parce qu'il crée de nouveaux usages et augmente considérablement la consommation numérique, le smartphone est devenu le principal allié du profilage publicitaire. Cet article propose quelques pistes pour en limiter quelques désagréments sur les plans environnemental (obsolescence logicielle retardée), éthique (contrôle des données), économique (financements non basés sur la publicité) et technique (logiciels plus performants car sans objectifs commerciaux).

LE MATÉRIEL

L'élément le plus fragile de votre téléphone est sans doute sa batterie. Le Conseil européen a adopté un règlement qui exige des constructeurs que les batteries soient facilement remplaçables à partir de 2027[1]. En attendant, choisir un modèle dont celle-ci est amovible, tel Fairphone, PinePhone, F(x) tec, Librem, etc. peut être un bon choix ; mais ces appareils nécessitent généralement un budget conséquent. Autrement, vous pouvez vous orienter vers un modèle dont vous trouverez la batterie vendue séparément ; si besoin, vous ferez confiance à un réparateur professionnel ou tenterez le remplacement vous-même à l'aide d'un tutoriel et d'outils spécifiques faciles à trouver[2]. Avec l'assurance de pouvoir changer la batterie, vous pouvez vous diriger vers des occasions reconditionnées sans trop de risques.

> Le monopole de Google sur le système d'exploitation renforce son monopole sur les applications et inversement.

LE SYSTÈME D'EXPLOITATION

En 2024, deux acteurs se partagent le marché des systèmes d'exploitation pour mobiles : Android de Google (70 %) et iOS d'Apple (28 %)[3]. Les autres acteurs, pourtant dominants sur les ordinateurs de bureau ou dans la construction de smartphones, comme Microsoft avec Windows Mobile ou Samsung avec son système Tizen, ne totalisent pas plus de 2 % de parts de marché. Google a écrasé ses concurrents avec un modèle économique inédit : Android, basé sur Linux, est open source et gratuit. Google gagne de l'argent avec les applications et services qu'il impose et avec son magasin d'applications Play Store dont il prélève 30 % des revenus. Le monopole de Google sur le système d'exploitation renforce son monopole sur les applications et inversement.

Par ailleurs, Android est assez vite dépassé. Les constructeurs supportent en effet rarement plus de deux ans leur matériel. Il est donc plutôt rare de pouvoir mettre son téléphone à jour deux ans après l'achat. Or, un téléphone non à jour est bien plus vulnérable, sujet aux dysfonctionnements, aux attaques virales et aux incompatibilités avec des applications. La disponibilité de systèmes d'exploitation alternatifs devrait donc être un critère déterminant dans le choix d'un smartphone.

LineageOS est certainement l'alternative la plus crédible et répandue au dominant Android, compatible avec quelque 200 smartphones. Son support vous offrira quelques années de répit supplémentaire passée la garantie du constructeur. Il s'agit d'un dérivé d'Android débarrassé des ajouts de Google, tout en maintenant une compatibilité matérielle optimale. Le site https://lineageos.org comprend une liste des modèles compatibles, ainsi que des tutoriels intelligibles pour effectuer l'installation.

Et si votre téléphone est également compatible avec **PostmarketOS**, vous retarderez l'obsolescence logicielle. Celui-ci est un système basé sur Linux comparable à ce que vous pouvez installer sur un ordinateur. Vous y retrouverez les mêmes applications, mais ne pourrez pas installer celles d'Android facilement. Ce système n'est, à l'heure d'écrire ces lignes, pas encore suffisamment mûr pour être utilisé au quotidien. Son évolution est néanmoins rapide et mérite d'être tenue à l'œil. Pour ce faire, parcourez la logithèque d'un système Linux et repérez les applications dont vous pourriez faire usage sur un smartphone. Il en existe bien plus que ce que l'on pourrait penser : même des applications bancaires sont en passe d'y apparaître.

LES MAGASINS D'APPLICATIONS

Sur Android et ses dérivés, vous n'avez pas l'obligation de vous créer un compte Google et de dépendre du bon vouloir de cette multinationale en situation de monopole. Vous pouvez, en effet, faire confiance à **F-droid**, un catalogue d'applications alternatif à Google Play Store donnant accès à une sélection rigoureuse de logiciels libres diminuant la fuite de vos données :

> La disponibilité de systèmes d'exploitation alternatifs devrait être un critère déterminant dans le choix d'un smartphone.

- **Firefox**, renommé **Fennec** sur F-droid, est le navigateur web le plus à même de contrer l'hégémonie de Google Chrome. En effet, le moteur de rendu Blink, soit l'une des pièces maîtresses de Chrome, par défaut sous Android est aussi celui de Microsoft Edge et d'Opera. Via ce nouveau quasi-monopole, Google impose sa façon de travailler aux développeur·euses et entrave régulièrement les extensions de blocages de publicités néfastes à son business[4]. Avec Safari d'Apple, Firefox est l'ultime rempart contrant la domination de Google dans ce domaine. Ajoutez-y **uBlock Origin** et **Privacy Badger** pour lutter contre la publicité et le traquage, **Multi account-containers** pour isoler des sites web (ainsi Facebook, par exemple, ne connaîtra rien des autres sites web que vous parcourez) ou encore **Cookie AutoDelete** qui accepte les cookies le temps de votre passage sur un site (sans quoi son fonctionnement s'en retrouve altéré) et les supprime à la fin de votre visite ; en association avec **I still don't care about cookies** pour éliminer les bandeaux d'informations de votre navigation désormais débarassée de cookies.
- **Organic Maps** fournit les cartes d'openstreetmaps.org avec un bon calculateur d'itinéraires piéton, vélo et voiture. L'application ne nécessite une connexion internet que pour télécharger les cartes de votre région, puis travaille sans connexion pour ne pas épuiser votre forfait de données mobiles. Son support des transports en commun est malheureusement encore très limité, mais cela pourrait évoluer très prochainement.
- **KeepassXC** enregistre vos mots de passe et vous aide à utiliser des mots de passes robustes et uniques pour chaque identifiant, augmentant grandement votre sécurité.
- **AntennaPod** et **NewPipe** vous permettent de suivre vos podcasts, chaînes Peertube, Youtube, Youtube Music, etc. sans publicités. Sur NewPipe, un mode *background* se limite au téléchargement de l'audio, rendant sa lecture bien plus économe en énergie et en données.
- **Aurora** pour accéder au catalogue de *Google Play* sans vous encombrer d'un compte Google et installer les rares applications dont on ne trouve pas encore d'alternatives libres crédibles.

LES FOURNISSEURS DE SERVICES

Un smartphone classique est lié à un compte Google ou Apple, proposant une large gamme de services synchronisés entre vos appareils et se nourrissant de contenus web : messagerie, stockage de fichiers, galerie photos, agenda, contacts, cartes, etc.

> Sur Android et ses dérivés, vous n'avez pas l'obligation de vous créer un compte Google et de dépendre du bon vouloir de cette multinationale en situation de monopole.

L'utilisation de ces services bien utiles s'accompagne de profilage publicitaire, traquage, etc. C'est pourquoi des associations et collectifs mettent à disposition l'infrastructure et les logiciels qui vous garantiront une plus grande souveraineté de vos données. CHATONS, le Collectif des Hébergeurs Alternatifs, Transparents, Ouverts, Neutres et Solidaires référence les structures répondant à une charte éthique. Parmi les membres de ce collectif, citons **Domaine Public**, partenaire de longue date d'IEB pour le support de son infrastructure informatique et d'une pléthore d'autres associations et collectifs ; ainsi que **Nubo**, coopérative belge offrant des services web aux particuliers.

Dans le cadre de cet article consacré au smartphone, attardons-nous sur Nubo – dont nous faisons une publicité assumée, car cette coopérative est une expérience unique en Belgique qui pourrait s'arrêter si elle ne rencontre pas plus d'adhérent·es.

Nubo, c'est avant tout une adresse mail que vous pouvez relier à votre smartphone et/ou ordinateur à l'aide de la messagerie **Thunderbird**. La mise en place a été grandement simplifiée : on entre son adresse, son mot de passe et c'est parti !

Nubo propose aussi le service **Nextcloud**, soit un espace en ligne pour conserver des fichiers, les partager ou y accéder à distance (à la manière de *Dropbox*). Depuis cet espace, vous pourrez sauver les photos de votre téléphone, éditer des textes collaborativement (alt. à Google Docs), créer des sondages de date (alt. à Doodle), gérer les dépenses d'un groupe (alt. à Tricount), sauver vos marque-pages, ou encore synchroniser agendas et contacts entre vos appareils (pour cela, installez **DAVx⁵** sur votre smartphone).

Avec Nextcloud, vous pouvez également enregistrer la configuration de tous les logiciels précédemment cités. Ainsi, vos mots de passe, votre liste de podcasts, vos chaînes vidéos, vos points géolocalisés, etc. peuvent être sauvés dans un répertoire de votre cloud assurant leur sauvegarde et lecture sur tous vos appareils, vous offrant un confort égalable à l'utilisation d'un compte Google ou Apple, mais en conservant le contrôle de vos données. ❏

1. Conseil de l'Union européenne, « Le Conseil adopte un nouveau règlement relatif aux batteries et aux déchets de batteries », communiqué de presse, 10 juillet 2023.
2. Le site web iFixit propose des tutoriels, des forums de discussion et des outils adaptés à chaque appareil [https://ifixit.com].
3. A. SHERIF, « Market share of mobile operating systems worldwide from 2009 to 2024, by quarter », www.statista.com, 23 septembre 2024
4. P. VAN LEEMPUTTEN, « uBlock Origin ne fonctionnera bientôt plus sur Chrome », *Le Vif*, 5 août 2024.

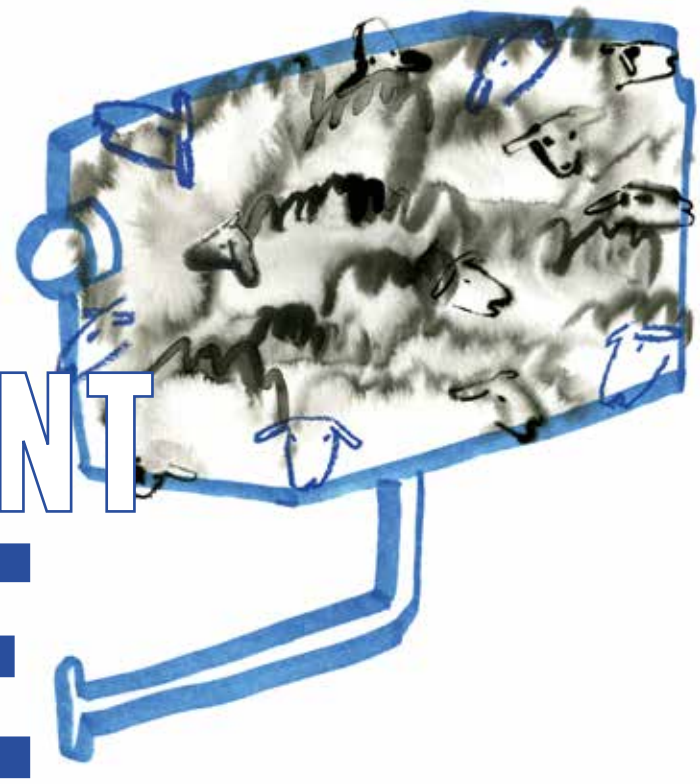
POUR ALLER PLUS LOIN

Divers groupes bruxellois peuvent vous aider concrètement dans la mise en place de ces alternatives : bxlug.be, nubo.coop et technopolice.be

Pour Android et dérivés
- **DivestOS** (alternative à Android) propose une page Applications recommandées en précisant quels sont leurs limites et points forts : https://divestos.org

Pour mobiles sous Linux
- **linuxphoneapps.org** référence des centaines d'applications que vous pouvez tester sur votre ordinateur Linux avant d'envisager l'installation d'un tel système sur votre téléphone.
- **Purism**, constructeur de smartphones open source, maintient une liste d'applications optimisées pour mobiles sous Linux : https://tracker.pureos.net/w/pureos/mobile_optimized_apps
- **Linmob** (Linux on mobile) résume, semaine après semaine, l'actualité logicielle et matérielle des systèmes Linux sur mobile et de ses applications : https://linmob.net

Toutes plateformes confondues
- **Framasoft**, association française de promotion du logiciel libre connue pour ses services Framadate, Framapad, etc. dispose d'un annuaire de logiciels libres, non-exclusivement orientés mobile, mais faisant référence en Francophonie : https://framalibre.org
- **AlternativeTo** est sans doute l'annuaire de logiciels le plus complet à ce jour, disposant de filtres open source, Android, Linux, etc. : https://alternativeto.net



DÉMOCRATIE & NUMÉRIQUE

COMMENT REPRENDRE LA MAIN ?

Comme tout dispositif technique, les dispositifs numériques sont pris dans un enchevêtrement complexe de représentations, d'acteurs et d'institutions qui déterminent leurs formes et leurs usages. Réseaux centralisés vs. décentralisés, logiciels libres vs. propriétaires, plateformes capitalistiques vs. communs coopératifs… La déclinaison peut être infinie. Néanmoins, la richesse de ce foisonnement ne doit pas faire oublier des rapports de force asymétriques.

Yaël Benayoun et Christelle Gilabert, Le Mouton Numérique

La numérisation n'est pas qu'une affaire de solution technique, mais un sujet de société à part entière.

En effet, il existe un numérique dominant dont les formes sont imposées par la poignée d'acteurs qui monopolise le marché. Cette mainmise n'est pas neutre ; elle a des conséquences directes sur les imaginaires, les normes et les modes de gouvernement.

UN NUMÉRIQUE DU DÉMANTÈLEMENT

Avec la micro-informatique, puis le big data, on observe la mise en place de politiques de management par la donnée dès les années 1980. Cela passe par tout un ensemble de dispositifs technologiques qui requièrent des formes de partenariats public-privé toujours plus intégrées… et déséquilibrées. Cela se traduit en effet par une externalisation massive des compétences et une dépendance des pouvoirs publics face aux entreprises qui détiennent l'expertise technique et savent s'imposer sur le marché.

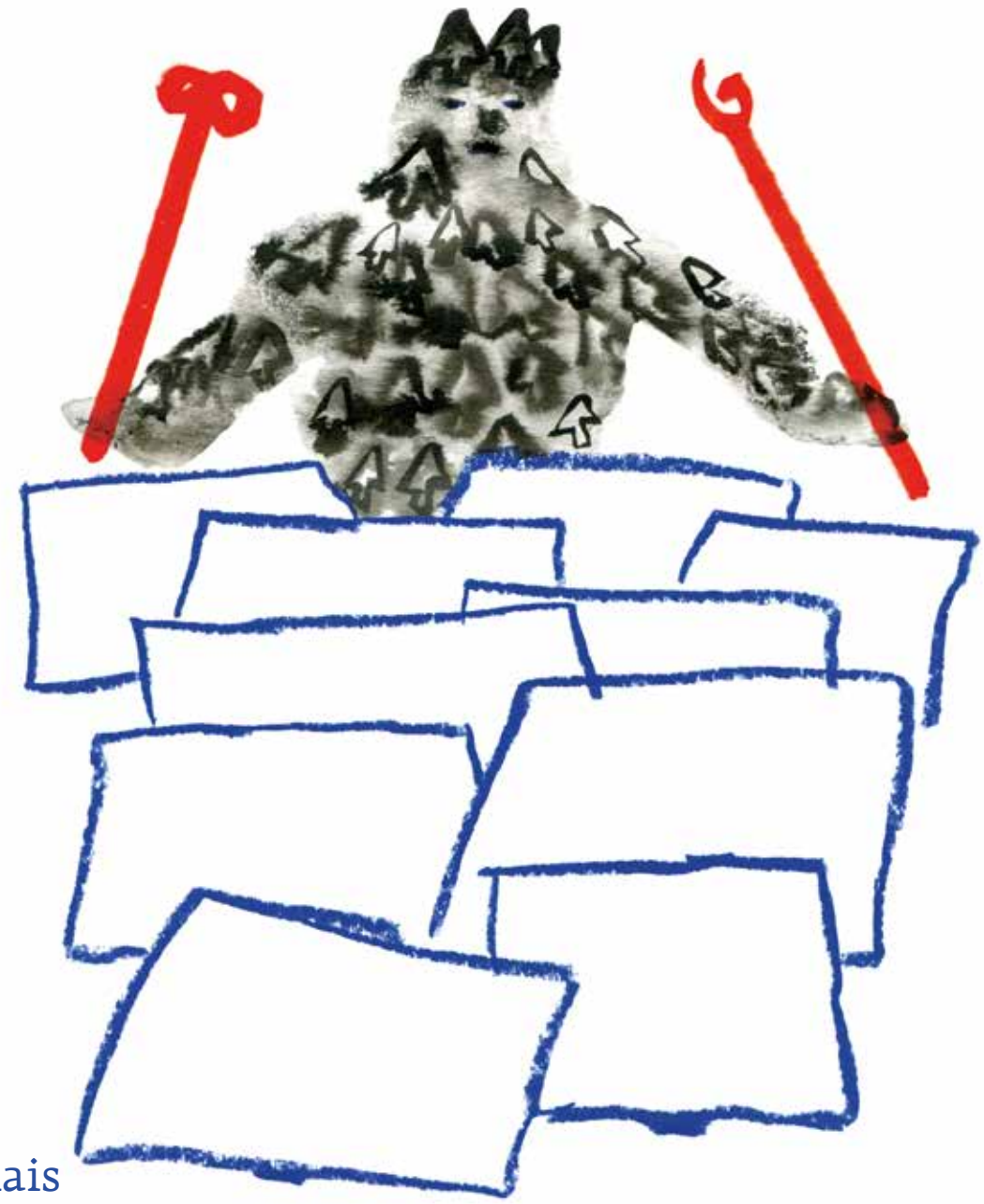
Le système numérique tel que nous le connaissons n'est qu'une version possible de son évolution.

Le cas de Sidewalk est éloquent. Sidewalk Labs est une agence d'innovation urbaine appartenant à Alphabet (ex-Google). Pour gagner le marché public lancé par la ville de Toronto pour la réhabilitation du quartier de Quayside, l'agence va jusqu'à promettre de construire à ses frais un institut d'innovation urbaine, d'ouvrir un fonds d'investissement pour les start-up locales ou encore une usine de bois massif, ce qui représenterait une économie estimée à 1,3 milliard de dollars canadiens pour la ville. Et cela ne s'arrête pas là. Sont également proposées des aides pour financer le développement des infrastructures numériques qui seront déployées dans le cadre de la réhabilitation, et le partage pendant vingt ans des bénéfices engrangés par ces mêmes infrastructures. Personne n'est dupe, les gains attendus reposent sur l'exploitation des données qui seront collectées par les capteurs de la ville. Mais dans un contexte budgétaire toujours plus contraint, comment refuser ?

Sidewalk est loin d'être un cas isolé[1]. Thalès use de stratagèmes similaires à Nice[2]. Les JO 2024 ont été le prétexte d'intenses tractations en faveur des lobbys sécuritaires[3]. Les grands cabinets de conseil[4] sont les premiers gagnants de la dématérialisation des démarches administratives… La liste est vertigineuse, tant le phénomène est structurel. Comment renverser le rapport de force ? Comment reprendre la main ?

CONTRE LA FATALITÉ NUMÉRIQUE

Le système numérique tel que nous le connaissons n'est qu'une version possible de son évolution. Une version qui résulte de choix politiques, économiques et industriels spécifiques. Elle correspond aux ambitions des grandes entreprises de la tech qui, avec le soutien des États, orientent les politiques publiques en leur faveur. Celles d'un numérique ultra-libéral qui répond à des logiques extractivistes, commerciales et sécuritaires. Le tout en invisibilisant les violences sociales et environnementales qu'il génère. Depuis des décennies, la façon dont le développement numérique est conduit échappe complètement à la société civile. Les citoyennes et les citoyens sont écartés du débat. Smartphones, réseaux sociaux, 5G, et maintenant Intelligence Artificielle… on leur impose sans cesse de nouveaux systèmes techniques au fonctionnement opaque, sur lesquels ils et elles n'ont aucune prise, que ce soit dans leur conception, dans leur gestion, ou dans leur accès. Malgré l'hégémonie des entreprises de la tech, cette configuration est loin d'être inéluctable. Cependant, elle nécessite de s'interroger collectivement sur la mise en œuvre de politiques numériques en phase avec les territoires et les populations.



Pas besoin d'être un·e expert·e pour exiger un système sain, transparent, et qui ne nuise pas à nos droits les plus fondamentaux.

DÉMOCRATISER LE DÉBAT NUMÉRIQUE

Au Mouton Numérique, nous appelons à «désingéniériser» les technologies. C'est-à-dire, à envisager le débat technologique au-delà d'une minorité d'expert·es et ingénieur·es, en ouvrant les discussions au sein du grand public. La numérisation n'est pas qu'une affaire de solution technique, mais un sujet de société à part entière. Car ces outils façonnent nos interactions au quotidien, en posant des questions d'ordre social. De la communication avec nos proches à l'accès aux services publics ou à l'information, la numérisation de nos activités est un processus profondément politique. Il affecte directement l'organisation de nos existences et de notre vivre-ensemble. Il est donc légitime d'avoir un droit de regard et de contestation lorsque ces systèmes nuisent au bien-vivre des personnes, ou bien à certains groupes. La numérisation devrait faire l'objet d'un débat public au même titre que l'alimentation, l'organisation du travail ou de la santé. S'interroger sur la conception des espaces, des outils et des infrastructures numériques, en prenant en considération leurs conséquences sur la vie des gens, serait la base d'une approche démocratique. Les expériences numériques concernent tout le monde, pas besoin d'être un·e expert·e pour exiger un système sain, transparent, et qui ne nuise pas à nos droits les plus fondamentaux.

Des collectifs militants congolais ont organisé des rassemblements devant les grandes boutiques d'Apple à travers le monde.

ÉCOUTER LES LUTTES POPULAIRES AUTOUR DU NUMÉRIQUE

Ces dernières années, les mobilisations contre les effets néfastes des technologies se multiplient à travers le monde. Contre la consommation des ressources, contre l'exploitation des travailleurs et des travailleuses, contre la surveillance des populations et la criminalisation des activistes, contre les cyberviolences. On voit apparaître de plus en plus de contestations contre l'implantation des datacenters : en Uruguay, aux Pays-Bas, en France, en Irlande. Ultra-consommateurs d'eau et d'énergie, ils sont accusés de mettre en danger l'approvisionnement des territoires concernés sans contreparties positives pour les habitantes et habitants sur place.

En février 2024, un collectif d'associations, dont Le Mouton Numérique, a signé une lettre ouverte au Premier ministre français Gabriel Attal[5] pour alerter sur les maltraitances institutionnelles liées à la dématérialisation des services de la CAF qui entravent dangereusement l'accès aux droits de ses bénéficiaires. À l'approche des JO de Paris, Amnesty International publiait au printemps 2024 une note intitulée *JO 2024 : Pourquoi la vidéosurveillance algorithmique pose problème ?*[6]. La publication visait à alerter sur les dangers d'une généralisation de la vidéosurveillance algorithmique qui menace «*le respect du droit à la vie privée et à la liberté d'expression*». Un problème pointé du doigt par le collectif citoyen Saccage 2024 un an plus tôt[7]. Enfin, encore plus récemment, à l'occasion de la sortie de l'iPhone 16 (septembre 2024), des collectifs militants congolais ont organisé des rassemblements devant les grandes boutiques d'Apple à travers le monde (Europe, États-Unis, Australie, Japon) pour dénoncer les atrocités de l'extractivisme minier qui sévissent dans la région du Kivu à l'Est de la République Démocratique du Congo. Ces rassemblements prenaient place dans le cadre d'une campagne mondiale de boycott de l'iPhone16. Ces exemples montrent les conséquences bien réelles, et parfois criminelles, de la numérisation et l'importance de faire du déploiement numérique un choix collectif et démocratique. Seulement, cela exige de créer les espaces de conscientisation et de discussion nécessaires pour pouvoir agir politiquement sur la façon de produire et gérer les vies numériques.

PENSER UNE FABRIQUE TERRITORIALE DU NUMÉRIQUE

Si le numérique échappe aux citoyennes et citoyens, il échappe également aux collectivités locales. Les grandes entreprises imposent leurs systèmes et infrastructures de façon uniforme sans réelle prise en compte des conditions des territoires. À l'image des data centers qui prolifèrent à travers le globe en consommant espaces et ressources au détriment d'autres usages locaux. Comme le montre le travail des chercheuses Fanny Lopez et Cécile Diguet : «*les réseaux du numériques se développent dans un âge post-services publics*» où le travail d'architecture des infrastructures pour assurer un développement dans l'intérêt général est complétement délaissé[8].

Or, les technologies numériques peuvent être adaptées au contexte géographique, social et culturel des territoires. Sur le plan politique, cela signifie les réintégrer dans une politique locale à partir des besoins et ressources disponibles. C'est toute la théorie de l'ingénieure-informaticienne espagnole Margarita Padilla – rapportée par la cyberféministe Alex Haché – qui établit un parallèle entre la souveraineté technologique et la souveraineté alimentaire[9]. Pour elle, il serait possible d'imaginer une production et une gestion des technologies relocalisées à l'échelle des territoires et des communautés. Même si elles sont minoritaires, de nombreuses alternatives numériques s'activent aux quatre coins du monde dans cette logique, prouvant que d'autres modèles sont possibles, pour développer et gérer les outils numériques en dehors des Big Tech. ➡

En France, on retrouve l'initiative Plateaux Numériques[10], qui est un programme d'accompagnement à destination des collectivités situées en zones rurales pour développer des sites web simples et durables adaptés à leurs contraintes (réseaux limités, équipements parfois obsolètes) tout en les formant à la gestion de ces services. Plus militantes, aux États-Unis, des associations de volontaires, comme le NYC Mesh, bricolent des réseaux informatiques locaux qui permettent d'accéder à Internet sans passer par les grands opérateurs commerciaux. Ces WiFi artisanaux donnent ainsi librement accès à Internet et à moindre coût pour les personnes défavorisées, et sans traçage de leurs données. Dans un monde où le numérique est omniprésent, cela permet de venir en aide à des populations précaires qui vivent dans des zones isolées ou bien dans des territoires qui traversent des périodes de crise (répression des autorités ou catastrophes naturelles). Autre exemple, en Espagne, où des collectifs féministes développent des serveurs numériques autogérés afin d'héberger des outils pour protéger les communications et les données de leurs luttes contre les risques d'attaques et de censures. C'est le cas du projet Anarchaserver[11] ou MaadiX[12].

Pas de surprises. Pour contrer un rapport de force, le plus efficace reste la lutte.

ALORS, PAR OÙ COMMENCER ?

Pas de surprises. Pour contrer un rapport de force, le plus efficace reste la lutte. On doit l'abandon du projet de réhabilitation du quartier Quayside de Toronto à l'intense mobilisation, de 2018 à 2020, du collectif d'habitantes et d'habitants Block Sidewalk. En 2019, les premières requalifications en contrat de travail de travailleur·euses de plateforme numérique sont une réponse aux actions répétées menées par des collectifs de chauffeurs VTC[13] ou de livreurs[14]. Plus récemment encore, l'interdiction de Airbnb annoncée par la ville de Barcelone s'inscrit dans le prolongement des luttes de collectifs militants pour le droit au logement, notamment la PAH[15].

Mais les luttes ne sont pas les seuls modes d'action permettant de concilier démocratie et numérique. Il existe tout un continuum. Tentative d'un rapide panorama *by* Le Mouton Numérique.

Parallèlement à l'analyse du cycle de vie (ACV) que l'on utilise pour réaliser le bilan environnemental « *multicritère et multi-étape* » d'un produit, il faudrait inventer l'analyse du cycle des décisions (ACD ?) ou des choix réalisés dans les différentes phases de vie d'un dispositif numérique. Autrement dit : regarder qui est impliqué dans quels choix, à quels moments et pour quoi faire. Cela fait ressortir un ensemble de « nœuds » sur lesquels agir.

Le premier, le plus évident, c'est le « nœud » des ingénieur·es, de celles et ceux qui font et conçoivent les dispositifs. Aujourd'hui, l'homogénéité de ce groupe est connue : massivement des hommes, cadres supérieurs, blancs. C'est comme ça qu'on se retrouve avec des savons automatiques qui ne reconnaissent pas les mains noires[16], seulement 400 langues présentes sur Internet[17] (vs. les 7 000 langues parlées dans le monde), des risques en moyenne 73 % plus importants d'être blessée dans un accident de voiture frontal quand on est une femme[18] ou à peine 13 % des sites publics accessibles aux personnes en situation de handicap[19]. Une solution simple et efficace pour remédier à ces situations, prônée par de nombreuses associations de personnes concernées : « Ne venez pas nous parler : embauchez-nous ! »

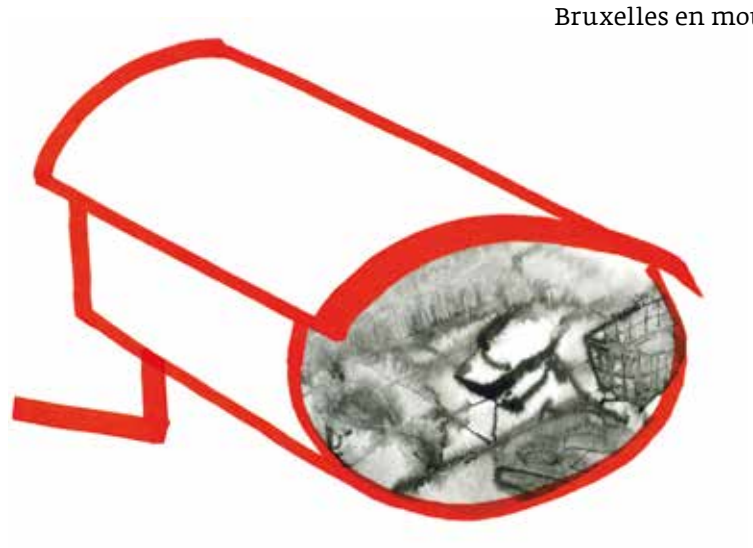
Regarder qui est impliqué dans quels choix, à quels moments et pour quoi faire. Cela fait ressortir un ensemble de « nœuds » sur lesquels agir.

ÉLARGIR LA SPHÈRE DES « EXPERTS »

Le second nœud est directement lié au premier : qui est considéré comme expert·e et à quels moments on les mobilise. Ce n'est pas un hasard si Callon, Barthe et Lascoumes conceptualisent la « démocratie technique » à partir des actions d'Act Up, association de lutte contre le VIH-Sida[20]. Dans les années 1980, internet permet l'émergence d'une « institution savante de fait »[21]. L'association fait valoir, face à l'autorité médicale et aux lobbys pharmaceutiques, un savoir expérientiel, c'est-à-dire un savoir scientifique enrichi du vécu des premières et premier·es concerné·es, en l'occurrence les personnes atteintes du VIH. Aujourd'hui, cet héritage se poursuit au sein de groupes féministes de réappropriation de savoir technique comme le festival La Tenaille[22], ou le Fluidspace[23], « *espace transféministe de rencontre, d'expérimentation et de hacking en tout genre* ».

Cette ouverture est le point de départ de la démocratie participative. À partir de là, plusieurs options sont possibles. Soit on ouvre les instances consultatives à d'autres types d'experts : en introduisant une « contre-expertise » via des collectifs de personnes concernées, d'acteurs de terrain, etc. Soit, de manière plus audacieuse, on modifie la constitution de ces instances par le tirage au sort par exemple. Cela signifie qu'on reconnaît les citoyennes et citoyens comme capables de produire une expertise scientifique. Le problème est que les espaces ainsi créés sont rarement connectés aux instances de décision et les propositions élaborées sont souvent décrédibilisées. Le détricotage en règle de la Convention citoyenne pour le climat n'illustre que trop bien ce phénomène.

Reconnaître les citoyennes et citoyens comme capables de produire une expertise scientifique.



REPRENDRE LE POUVOIR

Soit, de façon plus audacieuse encore, on change la composition des instances de décision : qui met les sujets à l'agenda, qui écrit les cahiers des charges et qui décide des solutions et orientations retenues. On a vu comment des hashtags comme *#metoo* parviennent à imposer dans le débat médiatique et politique des sujets et à entraîner l'ouverture de financements ad hoc. Mais on peut aller encore plus loin, à l'image des Pôles de citoyenneté expérimentés par l'Université Fédérale de Minas Gerais au Brésil[24]. Le programme développe des projets « d'extension universitaire » dans les communautés urbaines et les bidonvilles stigmatisés de Belo Horizonte. Inscrite dans la constitution brésilienne, l'extension universitaire est un impératif adressé à l'université d'aller se confronter aux populations locales. Dans les Pôles de citoyenneté, les communautés universitaires se mettent au service des communautés les plus pauvres pour améliorer leurs conditions matérielles de vie et favoriser leur émancipation. Les décisions sont prises en commun. Il y a ni sachant·es, ni expert·es : « *Les savoirs universitaires se démocratiseront et seront à leur tour enrichis par l'apport concret des communautés* ».

Ces formes de recherche-action gagneraient à être transposées dans le champ du numérique pour réintégrer les solutions déployées dans l'épaisseur du contexte social qui les reçoit. Des équipes mixtes de recherche en sciences sociales et ingénierie pourraient faire communauté avec des groupes ciblés par les contrôles algorithmiques par exemple. Réinterroger la pertinence des dispositifs techniques, comprendre les phénomènes sociaux et partir de la mobilisation des premières et premier·es concerné·es pour agir et construire ensemble des solutions. Il ne suffit pas de changer d'outils pour changer les rapports de pouvoir. L'émergence d'alternatives pérennes n'est possible que par l'intégration des savoirs numériques dans un tissu social plus dense. ❑

Réinterroger la pertinence des dispositifs techniques, comprendre les phénomènes sociaux et partir de la mobilisation des premier·es concerné·es pour agir et construire ensemble des solutions.

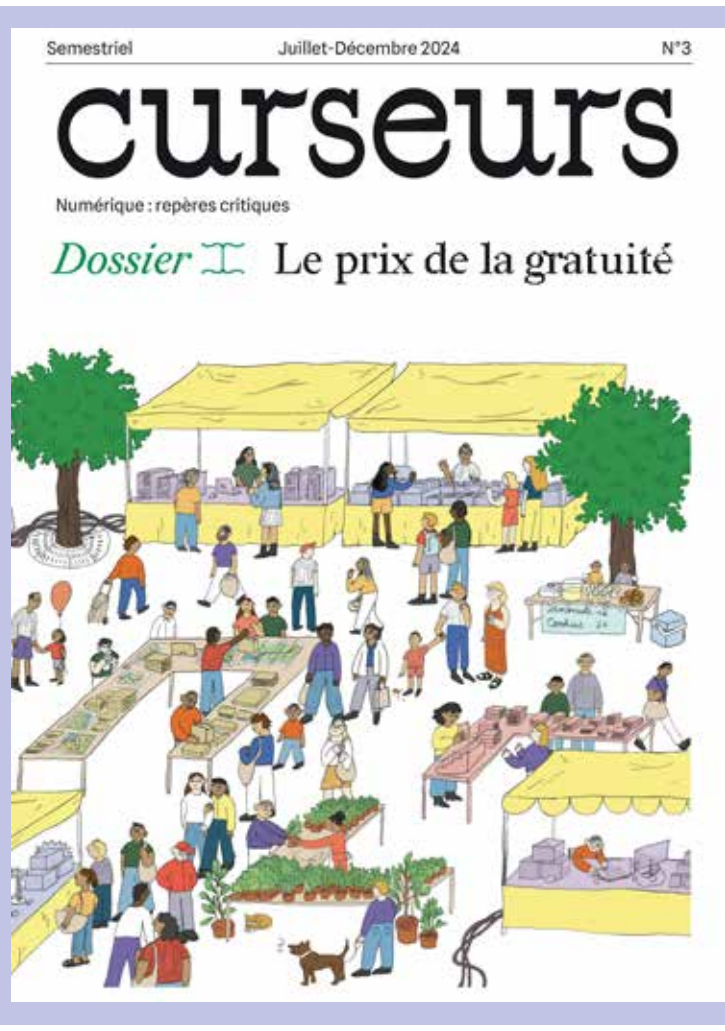
CURSEURS : LE PRIX DE LA GRATUITÉ

« Nous payons nos courses, nos trajets, nos loisirs et notre énergie. Nous achetons un ordinateur, un téléphone ou une tablette. Nous payons un accès à internet à la maison ou par les données mobiles… » Et sur internet, tout devient gratuit !

Si la gratuité s'est largement imposée dans le monde numérique, c'est parce qu'elle cache souvent un modèle économique fondé sur le traçage des utilsateur·ices à des fins de profilage publicitaire, par des entreprises qui assoient une position de monopole sur l'accoutumance à leurs services prétendument gratuits dont nous devenons les produits. Mais sur le web, la gratuité peut aussi être le fruit de propositions solidaires, respectueuses de la vie privée, fondées sur le bénévolat ou des modèles de financement alternatifs, participant d'un idéal de partage et motivée par la création de commun.

Cœur de son expérience en-ligne, la question de la gratuité constitue le dossier principal du numéro 3 du journal *Curseurs*, un semestriel engagé qui invite à penser les enjeux du numérique.

À lire sur papier et sur internet
https://www.curseurs.be/



1. Pour Bruxelles, voir aussi M. VAN CRIEKINGEN, « En cas de crise du logement, contactez votre administrateur système », *Bruxelles en mouvements* n° 281, février 2021.
2. C. LE FOLL et C. POURÉ, « Nice, le "little brother" de Thales », *Les Jours*, 19 novembre 2020 [https://lesjours.fr].
3. « JO 2024 : la frénésie sécuritaire », *La Quadrature du Net*, 15 octobre 2021 [https://www.laquadrature.net].
4. « Dématérialiser pour mieux régner », Le Mouton Numérique, 25 septembre 2022 [https://mouton-numerique.org].
5. « Lettre ouverte à Gabriel Attal – Utilisation d'un algorithme de ciblage et pratiques des CAF vis-à-vis de leurs allocataires », 6 février 2024 [https://changerdecap.net].
6. Amnesty International, « JO 2024 : Pourquoi la vidéosurveillance algorithmique pose problème », 15 avril 2024 [https://www.amnesty.fr].
7. Voir aussi S. D'HAENENS, « JO de Paris : le grand nettoyage social », *Bruxelles en mouvements* n° 330, juin 2024.
8. F. LOPEZ et C. DIGUET, *Sous le feu numérique*, éd. MetisPresses, 2023.
9. A. HACHÉ, « Le concept de la Souveraineté Technologique », *Ritimo.org*, 2014.
10. https://plateaux-numeriques.fr/
11. https://anarchaserver.org/
12. https://maadix.net/en/
13. Comme Capa-VTC et SCP-VTC (Syndicat des Chauffeurs Privés).
14. Comme le Clap (Collectif des livreurs autonomes des plateformes).
15. Plataforma de Afectadxs por la Hipoteca (Plateforme des victimes du crédit hypothécaire). Voir A. DEVILLÉ et C. SÉNÉCHAL « Espagne : La PAH (Plataforma de Afectadxs por la Hipoteca) », *Bruxelles en mouvements* n° 319, août 2022.
16. « This 'Racist soap dispenser' at Facebook office does not work for black people », *Futureism*, vidéo youtube, 18 août 2017.
17. État des lieux des langues d'Internet : https://internetlanguages.org/fr/
18. « *L'explication semble à trouver du côté des mannequins utilisés depuis des décennies dans les crash-tests automobiles par les pouvoirs publics et par l'industrie* ». Voir C. GAILLARD « Sécurité : À quand des femmes mieux protégées sur la route ? », auto-infos.fr, 1er mars 2023.
19. R. VALL, « Rapport d'information fait au nom de la mission d'information sur la lutte contre l'illectronisme et pour l'inclusion numérique (1) sur la lutte contre l'illectronisme et pour l'inclusion numérique », Sénat n° 711, 17 septembre 2020 [www.senat.fr].
20. M. CALLON, P. LASCOUMES et Y. BARTHE, *Agir dans un monde incertain. Essai sur la démocratie technique*, éd. Seuil, 2021.
21. A. CASILLI, « Le stéthoscope et la souris : savoirs médicaux et imaginaires numériques du corps », *Esprit* n° 3-4, 2009, p. 175-188.
22. https://latenaille.org
23. https://chloedesmoineaux.surf/fluidspace
24. « Le programme "Pôles de citoyenneté" » in A. RUBIÃO, « L'"extension universitaire" : une conception latino-américaine de la démocratisation de la connaissance », *Le sujet dans la cité* 2013/2 n° 4.

LA VIE PRIVÉE... POUR QUOI FAIRE ?

EXIGENCE DÉMOCRATIQUE ET RECONNAISSANCE FACIALE

Le recours, par l'institution policière, aux technologies de reconnaissance faciale fait aujourd'hui l'objet de vives discussions. Les lignes qui suivent entendent rendre à l'invocation du droit à la vie privée quelque chose de sa radicalité politique originale. L'auteur nous invite à concevoir le droit à la vie privée comme un moyen permettant de garantir effectivement la possibilité de résistance ou de désobéissance – ressorts essentiels de l'action politique dans des démocraties nécessairement imparfaites.

Jérôme Margnys

Le recours, par l'institution policière, aux technologies de reconnaissance faciale fait aujourd'hui l'objet de vives discussions. Ses défenseur·euses mettent généralement en avant : gains d'efficacité (réduction des taux de criminalité), diminution des coûts (baisse des effectifs policiers) ou amélioration des conditions de travail (dispensant les policier·es de fastidieuses enquêtes). Ses détracteur·ices leur opposent : une relative inefficacité (donnant lieu à des erreurs importantes de discrimination), une augmentation des coûts (licences logicielles, caméras haute définition et puissants serveurs) ainsi que des risques pour certains droits humains, notamment le droit à la vie privée – tel qu'il se trouve consacré par l'article 8 de la Convention européenne des droits de l'homme. Dans les lignes qui suivent, je m'attacherai à compliquer cette invocation du droit à la vie privée, souvent vague et dogmatique, afin de lui restituer quelque chose de sa radicalité politique originale. L'enjeu est au moins double. Contre l'invocation vague : esquisser quelques-uns des effets *concrets* de la reconnaissance faciale sur des situations sociales. Et contre l'invocation dogmatique : avancer des *raisons* de penser le droit à la vie privée comme un bien devant être préservé, plutôt que comme une contrainte devant être levée[1].

> Penser le droit à la vie privée comme un bien devant être préservé, plutôt que comme une contrainte devant être levée.

Précisons les termes. Les systèmes de reconnaissance faciale auxquels nous nous intéresserons articulent typiquement : (i) une base de données rassemblant des images de personnes, (ii) une base de données centralisant des flux de vidéo-surveillance, (iii) des algorithmes permettant de croiser, à des fins d'identification, les images contenues dans ces deux bases de données. En théorie, la police belge peut recourir aux technologies de reconnaissance faciale si et seulement si une disposition légale l'autorise explicitement à consulter des bases de données rassemblant des images de personnes à des fins de reconnaissance faciale. La seule base de données remplissant aujourd'hui ces conditions est une base de données européenne visant à faciliter les contrôles d'identité des demandeur·euses d'asile par les policier·es. En pratique, des enquêtes administratives, journalistiques et académiques ont permis d'établir que la police belge – aux niveaux local comme fédéral – a effectivement recouru, ces dernières années, à plusieurs reprises, à des systèmes de reconnaissance faciale, en dehors de tout cadre légal. Les avancées en matière d'analyse automatique d'image, le recours de plus en plus fréquent par la police à la reconnaissance faciale et la relative pauvreté des arguments avancés dans les discussions parlementaires nous imposent de réfléchir à ces enjeux politiques[2].

La reconnaissance faciale nous met d'abord face à un problème posé par la plupart des dispositifs répressifs. Ceux-ci cherchent généralement à accroître l'asymétrie de pouvoir entre gouvernants et gouvernés – schématiquement : *un* policier armé d'un fusil automatique peut plus facilement contraindre *plusieurs* individus. Le problème posé par ces dispositifs tient alors à la tension, à laquelle semblent confrontées la plupart des institutions politiques, entre exigences sécuritaire et démocratique. L'exigence sécuritaire pose la nécessité de la préservation des biens et des personnes. Elle se matérialise aujourd'hui, le plus souvent, par l'engagement d'effectifs policiers et l'acquisition de dispositifs techniques. Elle contribue, de fait, à creuser l'asymétrie entre gouvernants et gouvernés – sans laquelle la sécurité ne pourrait être garantie. L'exigence démocratique pose, idéalement au moins, l'identité des gouvernants et des gouvernés. Les décisions démocratiques seraient ainsi respectées, non pas tant en raison de l'effectivité d'un appareil répressif, qu'en raison de leur capacité à répondre de façon exigeante aux problèmes vécus par l'ensemble des personnes concernées. L'exigence démocratique semble, par contraste, associée à une relative symétrie entre gouvernants et gouvernés – sans laquelle la démocratie finirait par emprunter à la tyrannie ses moyens. La difficulté propre au raisonnement politique tient à la nécessité d'articuler ces deux exigences : démocratique et sécuritaire. ➡

> La police belge a recouru ces dernières années, à plusieurs reprises, à des systèmes de reconnaissance faciale, en dehors de tout cadre légal.

ABONNEZ-VOUS !

LE BEM, C'EST PAS UN CADEAU…

Le *Bruxelles en mouvements* (BEM), c'est une information située, des dossiers fouillés sur l'actualité bruxelloise en urbanisme et environnement et une lecture sociale de la ville. Notre bimestriel est distribué largement dans la ville, mais vous pouvez aussi vous abonner pour le recevoir directement dans votre boîte aux lettres.
Votre abonnement constituera un soutien précieux à la parution de notre journal et aux activités d'IEB. Si vous aimez le BEM, si vous pensez qu'une autre lecture de la ville est nécessaire et que celle-ci doit être diffusée, abonnez-vous !
https://civicrm.ieb.be/abonnez-vous/

La reconnaissance faciale nous met ensuite face à un problème posé par la plupart des dispositifs techniques. L'enjeu est ici de saisir l'ensemble des transformations sociales susceptibles d'être suscitées par de tels dispositifs. Nous sommes souvent amenés à porter notre attention sur ces quelques tâches, habituellement exercées par les humains, que les ingénieur·es semblent effectivement parvenir à déléguer à des dispositifs techniques – dans notre cas : une tâche relativement limitée de comparaison d'images. Le risque tient à ce que nous négligions une série d'autres transformations, notamment : l'écart entre les tâches effectuées par les humain·es et les tâches déléguées aux machines. Dans le cas des systèmes de reconnaissance faciale, cette transformation est au moins double. En premier lieu : l'automatisation permet de charger *un* système informatique de ce qu'autrement une *multitude* d'humains devraient faire. Elle limite le nombre d'humains nécessaires à l'exécution d'une telle tâche. En second lieu : l'automatisation stabilise l'exécution d'une directive qui aurait pu trouver, dans certains contextes, à ne pas être appliquée ou à être appliquée différemment. Les technologies de reconnaissance faciale ont donc bien pour caractéristiques essentielles d'accroître l'asymétrie entre gouvernant·es et gouverné·es et de limiter les possibilités de désobéissance.

Le problème se ramène alors à la question de savoir s'il est politiquement opportun de construire des espaces communs au sein desquels la résistance aux institutions devient pratiquement impossible. La difficulté tient dès lors à ce qu'il nous faut apprécier les rôles que peuvent jouer les mouvements de désobéissance ou de résistance – légaux ou illégaux, civils ou incivils – dans l'acquisition d'avancées sociales, morales et politiques. Historiquement, le mouvement américain des droits civiques, militant pour l'abolition des dispositions légales organisant la ségrégation raciale, illustre de façon particulièrement claire l'importance pratique de la possibilité de désobéir et de résister, afin de voir certaines luttes progresser. Politiquement, la résistance est souvent considérée comme légitime dès lors que les voies traditionnelles ne permettent pas aux institutions démocratiques d'entendre ou de prendre en charge certains des problèmes les plus criants et urgents vécus par leurs citoyen·nes. Dit autrement : il revient aux défenseur·euses de la reconnaissance faciale de montrer que celle-ci ne menace pas de priver les citoyen·nes de stratégies pourtant essentielles à nos vies démocratiques.

> Aux défenseurs de ces technologies de montrer que celles-ci ne mettent pas en péril certains des ressorts essentiels aux processus démocratiques.

« Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance. Ce droit englobe le droit à un nom, le droit au changement d'état civil et à une nouvelle identité, la protection contre les écoutes téléphoniques, la collecte d'informations à caractère privé par les services de sécurité d'un État et les publications portant atteinte à la vie privée. Ce droit permet aussi aux membres d'une minorité nationale d'avoir un mode de vie traditionnel [3]*. »*

Le droit à la vie privée m'intéresse ici surtout dans la mesure où il semble contribuer à la préservation, même minimale, des possibilités de désobéissance et de résistance vis-à-vis de nos institutions démocratiques. L'argument – s'il fait du droit à la vie privée un *moyen* plutôt qu'une *fin* – présente deux avantages, au moins. D'abord, il part de présupposés qui me semblent largement partagés, principalement : l'importance et la faillibilité des institutions démocratiques quant à l'organisation de la vie en commun. Ensuite, il contribue à renverser la charge de la preuve : il revient maintenant aux défenseur·euses de ces technologies de montrer que celles-ci ne mettent pas en péril certains des ressorts essentiels aux processus démocratiques. Pour autant, l'argument ne permet pas de conclure à la nécessité d'interdire la reconnaissance faciale : il nous impose par contre d'articuler – plutôt que de choisir – entre exigences sécuritaire et démocratique. Il est possible de reformuler ce qui vient d'être dit, de façon plus provocante. L'exigence sécuritaire ne serait en réalité pas assez ambitieuse : se concentrant exclusivement sur les gouverné·es, elle manque de voir que l'insécurité est parfois le fait des gouvernant·es. ❏

1. Les lignes qui suivent ne s'attardent donc pas sur les critiques visant son inefficacité ou son coût, dans la mesure où celles-ci ne concernent que peu la reconnaissance faciale : elles n'auraient pas grand chose à dire de systèmes ne faisant que peu d'erreurs ou ne représentant qu'un coût modeste.
2. Pour les rapports de l'Organe de l'Information Policière, voir : DIO19005 et DIO21006. Pour un article scientifique établissant l'usage de la reconnaissance faciale par la police belge, voir : L. ROOSELEERS et J. MAESSCHALK, « Digitalisering in de lokale politie in Vlaanderen en Brussel: Waar staan we? », *Panopticon* Vol. 42, no. 5, 2021, p. 419-438. Pour un article de presse discutant du recours à la reconnaissance faciale par la police belge, voir : F. DE HALLEUX, « Comme au procès Pélicot, la police belge utilise aussi un logiciel de reconnaissance faciale », *sudinfo.be*, 10 septembre 2024.
3. Article 8 de la Convention européenne des droits de l'homme.

Pour une Renolution publique du bâti bruxellois

➪ L'effet d'aubaine créé par les primes « Renolution » a été douché en plein été. Les propriétaires qui avaient engagé des travaux de rénovation et d'économie d'énergie ont en effet appris en juillet qu'il n'y avait plus un kopeck pour les soutenir financièrement. Les 69 millions d'euros prévus pour l'année 2024 avaient été octroyés. Une situation qui s'était déjà produite en 2023, mais l'exécutif avait alors pris la décision de renflouer les caisses. Impossible cette fois-ci d'effectuer une telle opération budgétaire puisque le gouvernement « sortant » est en affaires courantes.

Les autorités régionales ont donc suspendu, dès le 16 août, la possibilité d'introduire de nouvelles demandes de primes dans l'attente d'une décision du futur gouvernement bruxellois. Pour autant, l'obligation de rénovation pour les propriétaires de passoires énergétiques, elle, n'est pas suspendue. Le compte à rebours est enclenché : dès 2033, les bâtiments affichant une PEB F ou G seront « interdits » dans la capitale. Entendez : les propriétaires seront « punis » et devront s'acquitter de lourdes amendes.

En ce 25 septembre, à l'heure d'écrire ces lignes, la commission de l'Environnement du Parlement bruxellois a adopté à l'unanimité une proposition de résolution déposée par « *les partenaires potentiels francophones d'une majorité en Région bruxelloise (MR - Engagés - PS)* » visant à inciter le futur gouvernement régional à lever la suspension du versement des primes Renolution pour l'année en cours. Le texte demande au gouvernement « *de prévoir les moyens budgétaires nécessaires à la reprise du traitement des demandes de primes Renolution pour les travaux dont la facture de solde est acquittée d'ici au 31 décembre 2024 aux mêmes conditions qu'avant la suspension* ». Un ajustement budgétaire chiffré à 38 millions selon nos sources.

Force est de constater que l'enveloppe prévue pour inciter les propriétaires à rénover et isoler leur bien est insuffisante et ce, de façon récurrente. Or sans mettre un dispositif pérenne en place pour accompagner la stratégie Renolution, l'enveloppe sera toujours trop maigre. En mai 2023, BNP Paribas et le bureau d'études Profacts ont chiffré le budget nécessaire à la rénovation énergétique globale belge pour atteindre les objectifs européens à l'horizon 2050 à 300 milliards. Autre point noir à ce budget « primes » étriqué : même s'il veut équitablement inciter la rénovation énergétique, le dispositif échoue. Le rapport statistique annuel des primes énergie et Renolution tend à démontrer au fil des ans que les primes sont captées par les ménages à hauts revenus et cela même si les ménages à faibles revenus bénéficient en général d'une couverture de leur investissement supérieure aux autres catégories de revenus. La raison est simple : pour s'engager dans des travaux de rénovation, il faut du capital. À défaut, il faut emprunter de l'argent et recourir à des crédits à la consommation. Ecoreno, par exemple, même accessible aux seuls revenus médians et modestes, reste un crédit à la consommation.

Loin d'être une fatalité, la « faillite » du dispositif des primes est donc une belle occasion de penser d'autres modes de financement de la stratégie Renolution. Des outils économiques et sociaux pourraient être mis en place de façon combinatoire : un mécanisme de tiers payeur, une banque d'État, des régies communales autonomes, des rénovations par quartiers ou rues, le déploiement régional de réseaux de chaleur par rue, quartier ou îlot…

> Il semble urgent de penser la réduction de gaz à effets comme un engagement collectif soutenu de façon pérenne par l'État.

Ce qui semble urgent, c'est de penser la réduction de gaz à effets de serre non plus comme une charge individuelle qui incomberait à chaque ménage isolément mais comme un engagement collectif soutenu de façon pérenne par l'État. Des exemples fonctionnent à l'étranger. En Allemagne, la banque publique KFW (Kreditanstalt für Wiederaufbau – Établissement de crédit pour la reconstruction) accorde des prêts avec le dispositif du tiers payant pour la rénovation des logements. La banque prête et le remboursement se fait via la facture d'énergie. Ce dispositif a d'ailleurs été utilisé dans les années 1960 lors de l'installation du réseau de distribution de gaz dans les maisons bruxelloises des ménages modestes. L'ancêtre de Sibelga était alors le tiers payeur.

L'urgente rénovation du bâti bruxellois mérite un dispositif structurel, collectif et efficace.❏

Inter-Environnement Bruxelles

Bruxelles en mouvements est un bimestriel édité par IEB, fédération des comités de quartier et groupes d'habitant·es. Ce journal est distribué dans une série de lieux bruxellois, mais vous pouvez également vous abonner pour le recevoir à domicile et par la même occasion soutenir notre démarche.

Consultez notre site pour voir la publication en ligne ainsi que la liste des lieux de dépôt : www.ieb.be

Abonnement annuel (6 nos) : 24 euros
Abonnement de soutien : 50 euros
Versement au compte
IBAN : BE33 2100 0902 0446
BIC : GEBABEBB

Éditeur responsable : Patrick Wouters
Rue du Chimiste 34-36 – 1070 Bruxelles

Graphisme : Andreas Stathopoulos, Élise Debouny

Coordination : Matthias Förster, Benoît Coumont
Secrétaire de rédaction : Olivier Fourneau

Collaborateur·ices : Yaël Benayoun, Corentin Debailleul, Stéphanie D'Haenens, Christelle Gilabert, Maud Girault, Florence Huybrechts, Jérôme Margnys, Alice Querel, Martin Rosenfeld, Thyl Van Gyzegem

Illustrations : Théodora Jacobs [https://www.theodorajacobs.com/]

Inter-Environnement Bruxelles
Rue du Chimiste 34-36 – 1070 Bruxelles
Tél. : 02 801 14 80 – E-mail : info@ieb.be

Organisme d'éducation permanente soutenu par la Fédération Wallonie-Bruxelles

FÉDÉRATION WALLONIE-BRUXELLES